Steve W. Berman (*pro hac vice*)
Robert F. Lopez (*pro hac vice*)
HAGENS BERMAN SOBOL SHAPIRO LLP
1918 Eighth Avenue, Suite 3300
Seattle, WA 98101
Telephone: (206) 623-7292
Facsimile: (206) 623-0594
steve@hbsslaw.com
robl@hbsslaw.com

Bruce L. Simon (CSB No. 96241)
PEARSON SIMON & WARSHAW, LLP
44 Montgomery Street, Suite 1200
San Francisco, CA 94104
Telephone: (415) 433-9000
Facsimile: (415) 433-9008
bsimon@pswlaw.com

Plaintiffs' Interim Co-Lead Counsel

[Additional Counsel listed on Signature Page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

In re Carrier IQ, Inc. Consumer Privacy Litigation	No. 3:12-md-2330-EMC **PLAINTIFFS' MEMORANDUM IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS**
This Document Relates to: ALL CASES	Date: September 18, 2014 Time: 1:30 pm Place: Courtroom 5, 17th Floor Judge: Hon. Edward M. Chen

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES **PAGE(S)**

STATUTES

I. INTRODUCTION

Electronic communications, coupled with the power of the Internet, are a modern miracle. Only a few years ago, phones and tablets that enable one to exchange instant messages with his or her beloveds and friends; to meet someone new; to bank or buy books; to study a topic by searching the world's vast digital libraries; to find a political candidate's website; or to learn more about a medical concern—these were the stuff of science fiction. Now, though, tens of millions of consumers use their mobile devices daily to do all of that and more. This case is about the violation of Americans' rights to be free from unlawful interference and prying in the use of their smartphones and tablets—it is about the defendants' interception and manipulation of consumers' personal communications and data, including text messages, Internet search terms, and website user names and passwords; the defendants' unfair practices related to the widespread deployment of their privacy-infringing software; and the sale by device manufacturers of expensive phones rendered unmerchantable due to software that invaded consumers' privacy. Because plaintiffs have stated claims for violation of federal and state privacy laws, consumer protection acts, and federal and state warranty codes, defendants' motion should be denied.

II. STATEMENT OF RELEVANT FACTS

The privacy-infringing software here at issue has been installed on tens of millions of U.S. market mobile devices. (SCAC, ¶¶ 54-59, 77.) While touted as a product that helps wireless carriers offer better customer service, the software actually goes far beyond what carriers have said they wanted or evidently thought they had been provided. Not only does the software intercept consumer communications and private data, but in at least some installations, private content on affected devices has been transmitted to third-parties, including Google Inc. ("Google") and HTC, among possibly others. (SCAC, ¶¶ 73, 77.) As those who designed, pre-loaded, and made operable the software on plaintiffs' mobile devices, the defendants are responsible for the violations of law that plaintiffs allege.

A. American consumers learn of Carrier IQ Software

In the fall of 2011, millions of consumers heard for the first time of Carrier IQ Software. (SCAC, ¶ 40.) After publication of an initial batch of findings regarding the privacy-infringing

Carrier IQ Software he had found on his phone, Mr. Eckhart, an independent security researcher, published a more-detailed Part 2 of his work, both via his website and a 17 minute YouTube video released on November 28, 2011. In these follow-up publications, Mr. Eckhart expanded on his previous observations and demonstrated visually that Carrier IQ was intercepting communications and a significant amount of data and content, including keystrokes. He showed that the software was intercepting incoming SMS text messages, that is, SMS text message content in transit to the screen of the device. (SCAC, ¶ 46 and video referenced therein at 12:30 and 13:20 (place in video in minutes and seconds).) He also showed that the software was intercepting outgoing web queries and search terms, including those that should have been encrypted, given that they were sent via the secure HTTPS protocol. (*Id.* at 14:15, 14:55.) Worse, even when Mr. Eckhart was using his phone solely over Wi-Fi, rather than on a cellular network, he showed that the software was intercepting keystrokes and content, including outgoing HTTPS transmittals (carrying search terms), in unencrypted, human-readable form. (*Id.* at 13:35.) He also showed that on his installation, the data and content intercepted included: (a) HTTPS strings (carrying search terms), such as those created in HTTPS Google searches or HTTPS log-ins to PayPal, and (b) the content of SMS text messages, which additionally were being copied in unencrypted, human-readable text to his device's Android system log (which sometimes is referred to as a logcat log). (*See generally id.*; *see also* SCAC, ¶ 46.)

Once news broke widely of Mr. Eckhart's findings, Congress expressed deep concerns.[1] On November 30, 2011, U.S. Sen. Al Franken sent a letter to Carrier IQ, seeking answers to serious questions regarding its software. And on December 1, 2011, he followed up by sending letters to device manufacturers HTC, Motorola, and Samsung, and to wireless carriers AT&T, Sprint, and T-Mobile as well, seeking answers to the same sort of questions he had put to Carrier IQ. (SCAC, ¶ 48.)

[1] Later, the Department of Homeland Security ("DHS") issued a directive instructing police, fire, EMS, and security personnel to install an application that could "detect and remove the malicious software," *i.e.*, Carrier IQ Software. (July 23, 2013 Roll Call Release, Threats to Mobile Devices Using the Android Operating System, http://info.publicintelligence.net/DHS-FBI-AndroidThreats.pdf (last accessed June 22, 2014).) DHS categorized the Carrier IQ Software as rootkit software that "[l]ogs the user's locations, keystrokes, and passwords without the user's knowledge." (*Id.*)

The responses spoke to the widespread deployment of Carrier IQ Software. For example, Sprint indicated in its December 13, 2011 response to Sen. Franken that "[t]o the best of [its] knowledge, there are approximately 26 million active Sprint devices that have Carrier IQ Software installed." It stated that "[v]arious Sprint-offered devices manufactured by the following manufacturers have Carrier IQ Software installed: Audiovox, Franklin, HTC, Huawei, Kyocera, LG, Motorola, Novatel, Palmone, Samsung, Sanyo, and Sierra Wireless."[2] (SCAC, ¶ 54.)

As for HTC, it advised in its December 14, 2011 response that, "based on figures from wireless service providers, approximately 6.3 million HTC devices using the Carrier IQ Software are active devices." (SCAC, ¶ 57.) And Samsung, in its September 14, 2011 response, wrote that "STA has sold to carriers (and their distributors and agents) serving the U.S. market approximately 25 million total cell phones that were pre-installed with Carrier IQ Software." (SCAC, ¶ 58.)

B. Carrier IQ Software's interception and transmittal of private communications and content

The defendants—not only Carrier IQ, but the manufacturer defendants, too—designed and wrote components of Carrier IQ and installed the finished product on millions of mobile devices. Though the defendants contend that all of the plaintiffs' complaints are properly directed to the wireless carriers, in fact, the carriers say they never asked for or sought the private communications and content that defendants' software nevertheless intercepted and transmitted. (SCAC, ¶ 61.[3])

Carrier IQ designed, wrote, and caused the installation and activation of the Carrier IQ Software, including the so-called *IQ Agent*, on the devices at issue in this case. Carrier IQ also designed, authored, and provided guides to the defendant manufacturers so that they could design, write, install, and activate the *CIQ Interface* in deployments done by way of the so-called and most-

[2] Reportedly, Sprint began removing the Carrier IQ Software from mobile devices used on its network via over-the-air updates beginning in January 2012. Plaintiffs presently do not know if the software has been removed from all affected mobile devices operating on the Sprint network (though likely the software still resides on some consumers' devices, including those belonging to consumers who were no longer Sprint customers, and who therefore were unable to connect to Sprint's cellular network, at the time of the over-the-air updates). Nor do plaintiffs know if Sprint has re-deployed any Carrier IQ Software on any devices operating on its network. Also, plaintiffs do not know if the reported removal effected removal of all components of the Carrier IQ Software. (SCAC, ¶ 55.)

[3] Importantly, wireless carriers deny ever seeking information such as Internet search terms, text message content, or other private communications. (*See id.* and Sec. IV.B, *infra*.)

widespread "embedded" method of installation.[4] (*See, e.g.*, http://www.carrieriq.com /documents/understanding-carrier-iq-technology/6461/ (last accessed Aug. 17, 2014) ("CIQ White Paper") at 6).) Additionally, as part of its business model and as a function of the way its software is programmed, Carrier IQ can and does cause uploads of data collected on mobile devices either to its own servers or directly to the servers of its customers. (*E.g.*, CIQ White Paper at 11-13; SCAC, ¶ 62.)

The CIQ Interface is a wrapping or porting layer of code designed to see, recognize, and intercept a host of data and content, including SMS text message content and URLs containing search terms, user names, and passwords, among the other content described herein, and to send that material down to the IQ Agent for further processing and possible transmittals. (*E.g.*, CIQ White Paper at 6.) The manufacturers wrote the CIQ Interface with Carrier IQ's aid, and then the manufacturers installed it, as well as the IQ Agent—collectively, the Carrier IQ Software—on affected devices. (*See, e.g.*, *id.*; SCAC, ¶ 63.)

Thus installed, the Carrier IQ Software is able to, and does, intercept not only network diagnostic data such as the strength of radio signals, but also personal, private, confidential, and sensitive communications and content from the devices on which it is installed. The defendants, having designed, authored, programmed, and installed the components of the Carrier IQ Software, knew and intended what it would do. The manufacturers cannot claim that they simply installed an off-the-shelf product without knowing what it would do; they also wrote and installed software to intercept the laundry list of consumer communications, content, and data here at issue. (SCAC, ¶ 63.)

Carrier IQ Software operates in the background on affected devices. The typical user has no idea that it is running, nor can he or she turn it off, even as it stealthily infringes on his or her privacy and taxes the device's battery power, processor functions, and system memory. Also, unless consumers have advanced skills and are willing to root their devices and void their warranties, they cannot delete the software (and even those who have that skillset may be unable to remove it

[4] According to Carrier IQ, "Network Operators [the carriers] typically prefer the embedded version of the software as it provides the most comprehensive diagnostic set." (*See, e.g.*, CIQ White Paper at 6.)

completely). Furthermore, device owners were not given the choice of opting in or out of the software's functionality. (SCAC, ¶ 64; *see also id.*, ¶ 85 (discussing Android developer's conclusion regarding the Carrier IQ Software's diminishment of device performance and battery life).)

Not only did Mr. Eckhart and others show, but Carrier IQ admits, that the Carrier IQ Software intercepts data on mobile devices, including: URLs, including those containing HTTP and HTTPS query strings embedded with information such as Internet search terms (which could reveal a consumer's health conditions, sexual orientation, or other private information), user names, passwords, and granular, GPS-based geo-location information (even when a search is being conducted over Wi-Fi, rather than a mobile carrier's cellular network); granular, GPS-based geo-location information apart from that transmitted in URLs; SMS text messages; telephone numbers dialed and attached to calls received; other dialer keypad presses/keystrokes; and application purchases and uses, among other content. (*See, e.g.*, http://www.theverge.com/2011/12/5/2609662/carrier-iq-interview (last accessed Aug. 14, 2014) (December 5, 2011 interview with Carrier IQ's then V.P. of Marketing, Andrew Coward) ("Q. So we spent a while discussing SMS. What about HTTPS? We'd imagine that carriers might know which webpages you're going to, since they're providing your internet connection, but HTTPS is potentially a step beyond that. Sometimes you'll find website usernames, passwords and geolocation embedded in an HTTPS URL, things that we wouldn't normally expect our carrier to be looking at. A. It's a good question, *and it's important to highlight that kind of information is available*.") (emphasis added).) (SCAC, ¶ 65.)

Further, the Carrier IQ Software can and does capture and transmit device-specific identifiers, such that the foregoing information can be mated with a specific device. (*See, e.g.*, CIQ White Paper at 3; SCAC, ¶ 66.)

To reiterate, Carrier IQ Software is designed to intercept text message content. Carrier IQ acknowledges this, but claims that it is merely looking for certain codes that might be carried along with any message. Even if that were true, the Carrier IQ Software is intentionally designed to intercept all such content, unbeknownst to consumers. (*See, e.g.*, http://www.theregister.co.uk/2011/12/02/ carrier_iq_interview/?page=2 (last accessed June 20, 2014)

(December 2, 2011 interview with Andrew Coward, in which he states, in part: "With the SMS [text message] one, there are control messages that come to us through SMS. . . . So we look at SMS messages that come in . . . ."); *see also* http://www.theverge.com/2011/12/5/2609662/carrier-iq-interview (December 5, 2011 interview with Andrew Coward) ("Q. Do you feel that's happening now, that users have a good understanding of what information is being collected? A. Well, given the press over the past week, it suggests not . . . .").) (SCAC, ¶ 67.)

The consequences of the Carrier IQ Software's interception of so much data can be quite serious. In addition to the interception, capture, and transmittal of private and sensitive data, which has nothing to do with network diagnostics or improvement, deployment of the Carrier IQ Software has led directly to other grave breaches of privacy. (SCAC, ¶ 69.)

First, due to a purported programming error, AT&T admits that the Carrier IQ Software transmitted text message content to it. (SCAC, ¶ 70.) Second, in some deployments, including those on HTC mobile devices, a copy of data and content intercepted for Carrier IQ Software purposes also was sent in unencrypted, human-readable form to the system logs (sometimes called the logcat logs) of affected devices. The capture of this information in human-readable form, via so-called verbose logging, is starkly shown in Mr. Eckhart's YouTube video. (SCAC, ¶ 71.)

Once there, as recognized by the Federal Trade Commission ("FTC") in a Carrier IQ-related investigation (*see* Sec. II.C, *infra*), such content and data—SMS text messages; material including URLs embedded with HTTP/HTTPS query strings carrying web search terms and user names and passwords; and geo-location information, among other content and data—lies vulnerable to anyone with access to these logs, including those with malicious intent. Such information should not be captured in these logs, yet logging of such personal, private, confidential, and sensitive information has occurred on a massive scale.[5] (SCAC, ¶ 72.)

[5] HTC, the target of the investigation, used what Carrier IQ calls the most preferred method of installation of the software, *i.e.*, the embedded method. (SCAC, ¶ 77 (references by FTC speaking to embedded installation) and Sec. II.A, *supra*, n.4.) Given the preferred nature of this method, it is likely the installation method the other manufacturer defendants used as well. And given that Carrier IQ supplied the porting guides and specifications for the CIQ Interface to all manufacturers using the embedded method of installation, the devices of those other manufacturers may well exhibit the same sort of logging behavior that HTC's devices did (or do). (SCAC, ¶¶ 62-63, 77.) In fact, in another YouTube video, an individual demonstrates an in-development application meant to detect Carrier IQ Software. (https://play.google.com/store/apps/details?id=org.projectvoodoo.simplecarrieriqdetector&hl=en (last

Still worse, because device and application crash reports call on information stored in device logs, plaintiffs have confirmed via arbitration-related discovery in this matter that text message content, and possibly other confidential material and sensitive content captured in HTTP/S strings, was transmitted to Google, the owner and publisher of the Android OS, as part of, or along with, crash reports.[6] Additionally, per the FTC, HTC received such content by way of its Tell HTC tool, which draws on content stored in the device logs. (*See* Sec. II.C, *infra*.) Further, such content may have gone to application developers who draw on device logs as a means of diagnosing application crashes (or for other purposes). (SCAC, ¶ 73.) Again, these actions were the direct result of the deployment of the Carrier IQ Software on these devices, which was carried out jointly by Carrier IQ and at least one of the manufacturer defendants.

Finally, as Mr. Eckhart showed in his YouTube video, such activity is taking place on Carrier IQ Software-bearing devices even if the consumer is no longer a wireless carrier subscriber. So long as the software remains on the mobile device, it is functioning and transmitting as stated above (save for functions only relatable to cellular telephone service), even when the consumer is using the device solely on his or her private home Wi-Fi network. Mr. Eckhart showed a search query executed over Wi-Fi, including the search term, intercepted by the software (and subsequently logged to the device logcat log). (SCAC, ¶ 74.) Consumers were unaware of this happening on their Carrier IQ Software-bearing devices, due to the intentionally hidden nature of Carrier IQ Software, and it is one more reason why they would not have purchased these devices had they known they were bearing software that operated as alleged.

C. The FTC's investigation of, and actions against, HTC involving Carrier IQ Software

The FTC has investigated defendant HTC America, Inc. with regard to the Carrier IQ Software and related privacy and security flaws in the HTC mobile devices. Following this investigation, on February 22, 2013, HTC reached an Agreement Containing Consent Order with the FTC concerning serious security flaws that HTC introduced to its Android and Windows Mobile

accessed Aug. 21, 2014).) At 2 mins. and 19 secs. into his video, and at 3 mins. and 39 secs. into his video, he shows screens of the Samsung 4G Touch, and the Samsung Epic 4G, respectively, which show evidence of Carrier IQ Software in the devices' Android system logs (*i.e.*, logcat logs). As needed, plaintiffs respectfully request leave to amend their complaint to add references to this video.

[6] Plaintiffs confirmed this via arbitration-related discovery in this matter. (SCAC, ¶ 73.)

smartphones. After public comment, the FTC issued a Final Decision and Order on July 2, 2013 (although the Final Decision and Order itself is dated June 25, 2013). (SCAC, ¶¶ 75-76.)

In its press release on July 2, 2013, the FTC stated, *inter alia*, that HTC America, Inc. "failed to take reasonable steps to secure the software it developed for its smartphones and tablet computers, introducing security flaws that placed sensitive information about millions of consumers at risk." As part of the settlement agreement, HTC was prohibited from "making any false or misleading statements about the security and privacy of consumers' data on HTC devices." (SCAC, ¶ 76.)

In its Final Complaint, issued on June 25, 2013, in connection with the Final Decision and Order in the matter, the FTC alleged in part that HTC had "embedded Carrier IQ diagnostics software on approximately 10.3 million Android-based mobile devices and 330,000 Windows Mobile-based devices . . . ." It noted that "[i]n order to embed the Carrier IQ software on its mobile devices, HTC developed a 'CIQ Interface' that would pass the necessary information to the Carrier IQ software." The FTC also noted that among the "sensitive information being collected by the Carrier IQ software" was "GPS-based location information; web browsing and media viewing history; the size and number of all text messages; the content of each incoming text message; the names of applications on the user's device; the numeric keys pressed by the user; and any other usage and device information specified for collection by certain network operators . . . ." (SCAC, ¶ 77.)

Additionally, the FTC stated that when HTC was developing its CIQ Interface, it activated and left on at shipping time "debug code" that wrote the referenced information to Android system logs. Not only did this mean that sensitive information was left vulnerable to third-party applications (including crash-reporting applications), but also, according to the FTC, the material, "such as the contents of incoming text messages," could be and was accessed and sent to HTC itself via an HTC error reporting tool. (*Id.*)

The FTC also stated that "HTC's practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers." It concluded that "[t]he acts and practices of respondent as alleged in th[e] complaint *constitute unfair or deceptive acts or practices in or affecting commerce in*

violation of Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45(a)." (SCAC, ¶ 79 (emphasis added) (citations omitted).)

D. The plaintiffs

Plaintiffs hail from 13 states. Each alleges that his or her mobile device came with the Carrier IQ Software pre-installed. Each used his or her mobile device for web browsing and text messaging, including accessing, inputting, and transmitting confidential and sensitive information. None would have purchased his or her device had he or she known that the Carrier IQ Software and its components were installed and operating as alleged in the SCAC and taxing his or her device's battery, processor, and memory. (SCAC, ¶¶ 8-25.)

III. LEGAL STANDARDS

A. Fed. R. Civ. P. 12(b)(1) and Fed. R. Civ. P. 12(b)(6)

As this Court has recognized, under Fed. R. Civ. P. 12(b)(1), "a court may dismiss a complaint for lack of subject matter jurisdiction if the plaintiff cannot satisfy the standing requirements set by Article III of the U.S. Constitution." *Ross v. Sioux Honey Ass'n, Coop*, 2013 WL 146367, at *4 (N.D. Cal. Jan. 14, 2013) (citing *Chandler v. State Farm Mut. Auto Ins. Co.*, 598 F.3d 1115, 1121-22 (9th Cir. 2010)). "A jurisdictional challenge under Rule 12(b)(1) may be made either on the face of the pleadings or by presenting extrinsic evidence." *Id.* (citing *Warren v. Fox Family Worldwide, Inc.*, 328 F.3d 1136, 1139 (9th Cir. 2003)). Where, as here, the moving party asserts a facial challenge, the Court must accept all factual allegations in the complaint as true. *Id.*

A motion to dismiss under Fed. R. Civ. P. 12(b)(6) tests only the legal sufficiency of the claims asserted in a complaint. *Navarro v. Block*, 250 F.3d 729, 732 (9th Cir. 2001). Dismissal for failure to state a claim is "proper only where there is no cognizable legal theory or an absence of sufficient facts alleged to support a cognizable legal theory." *Id.* In deciding a motion to dismiss, the court must "accept the plaintiffs' allegations as true and construe them in the light most favorable to the plaintiffs." *Siracusano v. Matrixx Initiatives, Inc.*, 585 F.3d 1167, 1177 (9th Cir. 2009). A plaintiff need not plead "detailed factual allegations" to survive a motion to dismiss; the allegations must be "enough to raise a right to relief above the speculative level." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). This means that a complaint must contain "sufficient factual matter,

accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 570). The plausibility standard is not akin to a "probability requirement," but "simply calls for enough fact to raise a reasonable expectation that discovery will reveal evidence of [the claim]." *Twombly*, 550 U.S. at 556.

B. Fed. R. Civ. P. 9(b) does not apply to all of plaintiffs' claims.

Fed. R. Civ. P. 9(b) only applies to UCL and similar claims based on "fraudulent conduct." *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1125 (9th Cir. 2009); *Vess v. Ciba-Geigy Corp.*, 317 F.3d 1097, 1105 (9th Cir. 2003) (allegations of non-fraudulent conduct need only satisfy the ordinary notice pleading standards of Rule 8(a)). "[W]here a plaintiff alleges a unified course of fraudulent conduct and relies entirely on that course of conduct as the basis of that claim . . . the claim is said to be grounded in fraud or to sound in fraud, and the pleading . . . as a whole must satisfy the particularity requirement of Rule 9(b)." *McNeary-Calloway v. JP Morgan Chase Bank, N.A.*, 863 F. Supp. 2d 928, 960 (N.D. Cal. 2012) (internal quotations and brackets omitted).

However, Rule 9(b) does not apply to claims that are not grounded in fraud. For example, in *Vess*, the Ninth Circuit found that although the plaintiff alleged UCL and CLRA claims sounding in fraud, the plaintiff's allegations that the defendant "failed to warn consumers that the full range of Ritalin's side effects has not yet been adequately studied," "failed to disclose the limited effectiveness of its product," and "failed to disclose that the clinical literature on ADD/ADHD referred to in the DSM is of poor quality" were not grounded in fraud because they did not "rely entirely on a unified fraudulent course of conduct." 317 F.3d at 1105-06. Accordingly, Rule 9(b) did not apply to those claims. *Id.*

For those claims actually based in fraud, Rule 9(b) requires an "identification of the circumstances constituting fraud so that the defendant can prepare an adequate answer from the allegations." *Odom v. Microsoft Corp.*, 486 F.3d 541, 553 (9th Cir. 2007). The circumstances constituting the alleged fraud must "be specific enough to give defendants notice of the particular misconduct . . . so that they can defend against the charge and not just deny that they have done anything wrong." *Kearns*, 567 F.3d at 1124.

IV. ARGUMENT

A. Plaintiffs adequately allege Article III standing.

To establish a "case or controversy" under Article III, a party must have standing. *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs.*, 528 U.S. 167, 180-81 (2000). Specifically, the question of standing refers to whether a litigant is entitled to have the court determine the merits of a dispute. *Warth v. Seldin*, 422 U.S. 490, 498 (1975). To determine whether a party has standing, a court must determine whether the plaintiff has a "personal stake in the outcome of the controversy." *Carlough v. Amchem Prods.*, 834 F. Supp. 1437, 1446 (E.D. Pa. 1993). The Supreme Court has held that a plaintiff has the requisite "personal stake" if he or she can satisfy three requirements: (1) the plaintiff has suffered a concrete injury-in-fact ("injury-in-fact"); (2) the injury is fairly traceable to the challenged conduct ("traceability"); and (3) the injury is likely to be redressed by a favorable decision ("redressability"). *Id.*; *see also Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). Plaintiffs satisfy these requirements.

1. Plaintiffs have standing to assert their causes of action for violations of California Penal Code Section 502 and the state consumer protection statutes.

Plaintiffs have adequately alleged injury-in-fact to support Article III standing with respect to Cal. Penal Code § 502 and their claims for violations of the consumer protection statutes. Specifically, plaintiffs allege that: (1) they would not have bought their mobile devices had they known the Carrier IQ Software was installed and how it operated (SCAC, ¶¶ 8-25); (2) they have suffered degraded battery life and performance of their mobile phones (SCAC, ¶¶ 8-25, 85); and (3) with regard to HTC, that personal, private, confidential and sensitive communications are at risk of exposure to third-parties. (SCAC, ¶¶ 75-82.) These allegations of injury-in-fact support Article III standing.

For example, in *Goodman v. HTC Am., Inc.*, 2012 U.S. Dist. LEXIS 88496, at *3 (W.D. Wash. June 26, 2012), the plaintiffs alleged that the weather applications on certain HTC phones turned them into "surreptitious tracking devices." *Id.* The plaintiffs in *Goodman* also alleged that they would not have bought their phones, or would have paid less, had they known they were buying surveillance phones. *Id.* According to the court in *Goodman*, the plaintiffs pled a "'concrete and

particularized'" injury; specifically, the plaintiffs were "relieved of their money" by the defendant's deceptive conduct, namely, inadequate disclosures and omissions which "'affected Plaintiffs' and Class Members' decisions to purchase and willingness to pay a certain price'" for the phones. *Id.* at *15-16. Plaintiffs have made similar allegations here and, therefore, they have standing to sue.[7] (SCAC, ¶¶ 8-25.) Courts have repeatedly held that these types of alleged economic injuries are sufficient to establish standing. *See, e.g.*, *Pirozzi v. Apple, Inc.*, 966 F. Supp. 2d 909, 917 (N.D. Cal. 2013); *In re Google, Inc. Privacy Policy Litig.*, 2013 U.S. Dist. LEXIS 171124, at *24 (N.D. Cal. Dec. 3, 2013). Such "palpable economic injuries have long been recognized as sufficient to lay the basis for standing." *Sierra Club v. Morton*, 405 U.S. 727, 733-34 (1972); *see also San Diego Cnty. Gun Rights Comm. v. Reno*, 98 F.3d 1121, 1130 (9th Cir. 1996) ("Economic injury is clearly a sufficient basis for standing.").

With regard to plaintiffs' allegations of diminished battery life and performance, such allegations also support Article III standing. In *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040 (N.D. Cal. 2012), the plaintiffs alleged that the defendants unlawfully allowed third-party applications to run on the iPhone, iPad and iPod Touch and use, for commercial purposes, personal information without user authorization or knowledge. *Id.* at 1049. In the *iPhone Application Litig.*, the district court held that allegations of diminished mobile resources, which were less detailed than those here, were sufficient to support Article III standing. *Id.* at 1054.

Similarly, the court in *Goodman* found allegations of battery discharge sufficient to meet the injury-in-fact requirement where the application at issue sent "fine" location data (accurate to identify a customer's location within a few feet) every three hours or whenever the device's screen was refreshed. 2012 U.S. Dist. LEXIS 88496, at *18-19. In *In re Google Android Consumer*

[7] Defendants seem to argue that these "overpayment" allegations (which defendants refer to as "benefit of the bargain" injuries), are insufficient to support standing because plaintiffs purportedly have not established a causal connection between the injury and the alleged misconduct. (Defs' Consol. Mot. To Dismiss ("Mot.") at 15-17.) According to defendants, plaintiffs have not identified any representations or omissions by them that could support reliance. (Mot. at 15.) Plaintiffs address this issue in Sec. IV.A below. In any event, plaintiffs' consumer protection claims are not simply based on conduct that is fraudulent or likely to deceive reasonable consumers. The UCL prohibits conduct that is "unlawful, unfair or fraudulent," and plaintiffs allege that defendants violated all three prongs. (SCAC, ¶ 117.) Plaintiffs do not have to show reliance under the unlawful or unfair prongs, and therefore, defendants' standing arguments fail. *See In re Tobacco II Cases*, 46 Cal. 4th 298, 326 n.17 (2009) (noting that the reliance requirement under the UCL is limited to claims involving false advertising and misrepresentations and there are many types of unfair business practices where the concept of reliance has no application).

Privacy Litig., 2013 U.S. Dist. LEXIS 42724, at *17 (N.D. Cal. Mar. 26, 2013), the court found allegations of battery depletion sufficient for standing based on allegations that the "batteries discharged more quickly[,] and that their services were interrupted." And in *Google Inc. Privacy Policy Litig.*, the Court found standing based on allegations that battery consumption occurs each time a user downloads any application. 2013 U.S. Dist. LEXIS 171124, at *21.

Like the plaintiffs in the above cases, plaintiffs here have adequately alleged injury-in-fact based on performance and battery degradation. (SCAC, ¶¶ 2-25, 74, 85.) Additionally, with regard to HTC, plaintiffs' allegations that their sensitive and personal communications are not secure and are at risk of exposure are sufficient to support injury-in-fact. *See iPhone Application Litig.*, 844 F. Supp. 2d at 1055; *see also Covington v. Jefferson Cnty.*, 358 F.3d 626, 638 (9th Cir. 2004) (holding that increased risk of injury constitutes cognizable harm for the injury-in-fact requirement); *Central Delta Water Agency v. United States*, 306 F.3d 938, 947 (9th Cir. 2002) (same); *Hall v. Norton*, 266 F.3d 969, 976 (9th Cir. 2001) (same). The severity of the plaintiff's injury is immaterial, and as the Supreme Court has stated, an "identifiable trifle" of injury may provide the basis for standing. *United States Students Challenging Regulatory Agency Procedures (SCRAP)*, 412 U.S. 669, 690 (1973).

Defendants nevertheless argue that such allegations do not suffice. They rely on *Opperman v. Path, Inc.*, 2014 U.S. Dist. LEXIS 67225 (N.D. Cal. May 14, 2014) and *Hernandez v. Path, Inc.*, 2012 U.S. Dist. LEXIS 151035 (N.D. Cal. Oct. 19, 2012). Defendants are wrong. The reason allegations of diminished battery life were insufficient in *Hernandez* is because the reduction in battery usage was only for "two to three seconds," upon a person's downloading of an application. *Id.* at *4. According to the court in *Hernandez*, such diminished battery life was *de minimis*. *Id.* *Opperman* similarly found that the allegations of diminished battery life were insufficient to support standing because they were not detailed but generalized. *Id.* at *81. The court in *Opperman*, however, did recognize that if battery usage was significant and systemic, the allegations could support standing. *Id.*

In contrast to *Hernandez* and *Opperman*, plaintiffs' allegations of diminished performance and decreased battery life are significant and systemic. Plaintiffs allege that the Carrier IQ Software

runs on mobile devices continuously. (SCAC, ¶¶ 74, 85.) Further, plaintiffs allege that the Carrier IQ Software cannot be turned off, and that they and class members are not getting the optimal performance of the mobile devices they purchased, and which are marketed, in part, based on their speed, performance and battery life. (*Id.*, ¶ 85.) Further, Android developer, Tim Schofield, has gone on record stating that the presence of Carrier IQ Software "necessarily degrades the performance of any device on which it is installed." (*Id.*) Plaintiffs also allege that the reduction in battery life and performance can be proven. (SCAC, ¶ 106.) These allegations, which must be accepted as true, are definitely more than sufficient to meet the injury-in-fact requirement.[8]

Defendants' arguments that alleged security vulnerabilities are insufficient to meet the injury-in-fact requirement also ignore plaintiffs' allegations. *See Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1126 (N.D. Cal. Mar. 2008) (allegations that plaintiff suffered from an increased risk of identity theft due to theft of laptops containing personal information were sufficient at pleading stage to confer standing). The Ninth Circuit has addressed the issue of when the risk of a future harm may give rise to an injury-in-fact. In *Hartman v. Summers*, 120 F.3d 157, 160 (9th Cir. 1997), the court stated that to "confer standing, the threat of future injury must be credible rather than remote or hypothetical." *Id.* Thus, a plaintiff "must show a very significant possibility that the future harm will ensue." *Id.*

Unlike the facts in the cases cited by defendants, plaintiffs' allegations here rise beyond a hypothetical nature or mere speculation. Specifically, according to the FTC's Final Decision and Order dated July 2, 2013, HTC failed to take reasonable steps to "secure the software it developed for its smartphones and tablet computers, introducing security flaws that placed sensitive information about millions of consumers at risk." (SCAC, ¶¶ 76-82.) Further, as a result of HTC's conduct, highly sensitive information, such as web browsing and media viewing history, the content of text messages, and GPS-based location information was actually intercepted and accessible to third-party applications on user devices. (SCAC, ¶¶ 77, 81.) This increased and unreasonable risk to the security of sensitive personal information is credible, as even the FTC took action against HTC, and therefore sufficient to confer standing at this stage.

[8] There is no requirement that plaintiffs allege they had to replace the batteries, buy additional memory or pay other out-of-pocket expenses. (Mot. at 13:24-26.) Plaintiffs' economic injuries are evident based on their detailed allegations of performance degradation. (SCAC, ¶¶ 74, 85, 106.)

2. Defendants' arguments regarding whether plaintiffs have standing under other state laws and against defendants with whom they have had no dealings are premature.

Defendants do not dispute the standing of the named plaintiffs under their home state laws. Instead, they seek to dismiss the claims of class members in 35 states where no named plaintiff resides under the guise of standing. (Mot. at 9.) "While '[o]rdinarily . . . any . . . Article III court must be sure of its own jurisdiction before getting to the merits,' exceptions may be made in class actions where the class certification issues are 'logically antecedent' to Article III concerns." *Jepson v. Ticor Title Ins. Co.*, 2007 U.S. Dist. LEXIS 53480, at *3-4 (W.D. Wash. May 1, 2007) (quoting *Ortiz v. Fibreboard Corp.*, 527 U.S. 815, 831 (1999) (analyzing class certification before standing in the context of a mandatory global settlement class)).

This is one of those cases where an exception should be made because the "class certification issue is logically antecedent to Article III standing where the standing concerns 'would not exist but for the class-action certification.'" *Jepson*, at *4 (citing *Amchem Prods. v. Windsor*, 521 U.S. 591, 612 (1997)). As the court in *Jepson* found, if the Court here determines that class certification of the various state claims is appropriate, "there is no question that the proposed class would have standing to assert non-Washington claims[.]" *Jepson*, at *4. "In such cases, 'it is possible for . . . common issues to predominate and for class certification to be an appropriate mechanism for handling the dispute.'" *Id.* In fact, a number of courts have found that it is more appropriate to decide class certification first, followed by any Article III challenges. *See Jepson*, at *4; *see also Donohue v. Apple, Inc.*, 871 F. Supp. 2d 913, 922-23 (N.D. Cal. 2012); *Hydroxycut Mktg. & Sales Practices Litig. v. Iovate Health Scis. Grp.*, 801 F. Supp. 2d 993 (S.D. Cal. 2011).

As the court in *Ramirez v. STi Prepaid LLC*, 644 F. Supp. 2d 496, 505 (D.N.J. 2009) explained:

> Defendants' argument appears to conflate the issue of whether the named Plaintiffs have standing to bring their individual claims with the secondary issue of whether they can meet the requirements to certify a class under Rule 23 . . . the fact that the named Plaintiffs may not have individual standing to allege violations of consumer protection laws in states other than those in which they purchased Defendants' calling cards is immaterial. The issue Defendants raise is one of predominance—whether 'questions of law or fact common to class members predominate over any questions affecting only individual members.'

Id.

Here, the defendants' conduct was uniform and, given the ubiquity of cell phones, most assuredly affected consumers in every U.S. jurisdiction in a similar fashion—the question of whether named plaintiffs have standing to assert claims on behalf of the class, including those residing in other states, is therefore more appropriately determined at class certification, not as part of standing on a motion to dismiss. *See In re Grand Theft Auto Video Game Consumer Litig.*, 2006 U.S. Dist. LEXIS 78064 (S.D.N.Y. Oct. 25, 2006); *see also In re Bayer Corp. Combination Aspirin Prods. Mktg. & Sales Practices Litig.*, 701 F. Supp. 2d 356, 377 (E.D.N.Y. 2010); *In re Pharm. Indus. Avg. Wholesale Price Litig.*, 252 F.R.D. 83, 104 (D. Mass. 2008) ("In a multi-state class, the caselaw does not create a *per se* rule that the Court must appoint a separate representative for each state or even each group.") (citations omitted).

Considering class certification issues first, followed by any standing issues, is not contrary to the Ninth Circuit's decision in *Easter v. Am. W. Fin.*, 381 F.3d 948 (9th Cir. 2004). As the court in *Jepson* explained, the Ninth Circuit in *Easter* held that the named plaintiffs lacked standing to sue certain defendants since they could not trace their injuries to them, even though the defendants had behaved in similar fashion to others who had caused traceable injuries to the named plaintiffs. *Jepson*, 2007 U.S. Dist. LEXIS, at *5 (citing *Easter*, 381 F.3d at 956, 962). Here, as in *Jepson*, plaintiffs allege injuries traceable to defendants and "merely purport to represent a class of those similarly injured by [defendants] under analogous laws in other states." *Jepson*, at *5. As the court found in *Jepson*, addressing class certification before standing is clearly warranted, and while "*Easter* indicates that there is no *per se* rule that class certification must be considered before standing issues, it does not—and cannot—stand for the proposition that standing always has to be considered first." *Id.*[9]

Similarly, defendants argue that plaintiffs have no claims against "any OEM

[9] The cases cited by defendants either applied *Easter* unnecessarily broadly, or did not thoroughly consider whether class certification issues are logically antecedent to Article III issues. *See, e.g., In re Flash Memory Antitrust Litig.*, 643 F. Supp. 2d 1133, 1164 (N.D. Cal. 2009) (plaintiffs did not contest standing issues and requested leave to amend to join plaintiffs in states where named plaintiffs did not reside); *Pardini v. Unilever United States, Inc.*, 961 F. Supp. 2d 1048, 1061 (N.D. Cal. 2013) (did not analyze whether class certification was logically antecedent to standing); *In re Apple AT&TM Antitrust Litig.*, 596 F. Supp. 2d 1288, 1309 (N.D. Cal. 2008) (same); *In re Aftermarket Auto. Lighting Prods. Antitrust Litig.*, 2009 WL 9502003, at *22 (C.D. Cal. July 6, 2009) (interpreting *Easter* broadly); *In re Ditropan XL Antitrust Litig.*, 529 F. Supp. 2d 1098, 1107 (N.D. Cal. 2007) (same); *In re Graphics Processing Units Antitrust Litig.*, 527 F. Supp. 2d 1011, 1026-27 (N.D. Cal. 2007) (same).

other than the one that manufactured his or her phone." (Mot. at 11.) Each of the OEM defendants, however, is properly in the suit because there is at least one named plaintiff who bought a mobile device manufactured and/or distributed by each OEM.

3. Plaintiffs Cribbs and Pipkin have adequately alleged injury-in-fact.

Defendants argue that the claims of plaintiffs Cribbs and Pipkin should be dismissed because, according to defendants, they have alleged contradictory statements regarding standing. This is not true. Plaintiffs Cribbs and Pipkin specifically allege that the "Carrier IQ Software and related implementing or porting software was installed and operating on [their] device[s], and taxing [their] device[s'] battery, processor, and memory." (SCAC, ¶¶ 9, 17.) The allegation that defendants actually point to—that Carrier IQ Software "also is embedded on the HTC Vivid, LG Nitro and Samsung Skyrocket devices, but has not been activated due to the potential for the software agent to interfere with the performance of those devices"—is actually a quote from AT&T's December 14, 2011 letter to Sen. Franken, and not a factual allegation from plaintiffs' experience or their counsel's investigation, which is ongoing. (SCAC, ¶ 53.)

B. Plaintiffs allege claims adequately under the Federal Wiretap Act.

Carrier IQ *and* the manufacturer defendants wrote and caused the installation of software on millions of mobile devices that admittedly is designed to gather and sometimes transmit a host of user communications and data to others. For purposes of preserving their Federal Wiretap Act claims against defendants' motion to dismiss, plaintiffs focus on SMS text messages, Internet search terms, user names and passwords, and whatever else may have been contained in or appended to HTTP/S URLs, though in fact the software intercepted much more. These constitute communications that the defendants *intentionally* intercepted—not only Carrier IQ understood and intended these communications, but so did the device manufacturers. How so? Because as Carrier IQ indicates, in order to effect the most popular installation of its software, n.4, *supra*, the manufacturers wrote the very software that intercepted, gathered, and passed down these communications for further processing. (SCAC, ¶ 63.) In reality, where consumers are concerned, the manufacturers' conduct was even worse that Carrier IQ's. It is the manufacturers' devices that consumers spent much of their hard-earned money buying, and yet these manufacturers knowingly

and intentionally installed privacy infringing software on those same devices, thereby causing the interception of their own customers' private communications. It bears repeating: this is no off-the-shelf product that manufacturers installed; they participated in programming components of it with the express purpose of making it do what is complained of in this lawsuit. What is more, none of the defendants can point to the carriers as the real culprit here—the carriers have said that *they did not seek the interception and transmittal to them of the content of plaintiffs' private communications*. (*See* Declaration of Tyler G. Newby in Supp. of Defs' Consol. Mot. To Dismiss ("Newby Decl.") (Dkt. No. 304-3) Ex. 1 at 2-4 (statement of AT&T to Sen. Franken that it did not intend to receive either the contents of text messages sent or received, or the contents of users' online search queries); Ex. 2 at 3 (statement of Sprint to Sen. Franken that it did not receive either the contents of text messages sent or received, or the contents of users' online search queries).) Rather, this suit is about *defendants*' conscious and intentional choices. Plaintiffs' claims, therefore, survive defendants' motion to dismiss.

1. Plaintiffs adequately allege the interception of contents of communications within the meaning of the Federal Wiretap Act.

Defendants contend that plaintiffs do not allege acquisition of contents of communications that was contemporaneous with their transmission. Accordingly, defendants contend, plaintiffs' Federal Wiretap Act claims should be dismissed. But defendants are wrong; plaintiffs have adequately alleged interception of contents of electronic communications.

a. Plaintiffs allege adequately interception contemporaneous with transmission.

Plaintiffs allege interception of contents of electronic communications, including SMS text message content, Internet search terms, and user names and passwords. (*See, e.g.*, SCAC, ¶¶ 46, 63, 65, 67, 77.) These claims are adequate to allege that contents of electronic communications were intercepted by defendants via "acquisition contemporaneous with transmission." *See Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 876-79 (9th Cir. 2002) (juxtaposing acquisition of "stored electronic communication(s)" with acquisition of electronic communications contemporaneous with transmission, the latter being actionable under the Federal Wiretap Act). Additionally, Mr. Eckhart's YouTube video, which is referenced in the SCAC, shows dynamic interceptions of: incoming SMS

text message content transmitted over a cellular network while the message is en route to the user[10]; outgoing HTTPS search terms transmitted over a Wi-Fi connection; Internet search terms transmitted over a cellular network; and user names and passwords transmitted over a cellular network. (SCAC, ¶¶ 65, 74.) There is no suggestion whatsoever from the plaintiffs in the SCAC—or the defendants—that any of this content was accessed while in storage or not while in transit. Indeed, in the *Register* interview of Carrier IQ's then vice-president, cited in the SCAC, Mr. Coward states as follows: "We receive this information *in real time, so a text message comes in, we'll look at it*. Is it for us? No, discard." (*See* http://www.theregister.co.uk/2011/12/02/carrier_iq_interview/?page=2 (last accessed Aug. 18, 2014) (December 2, 2011 interview with Andrew Coward) (emphasis added) (interview cited in SCAC, ¶ 67).)

Here, plaintiffs allege that the software, including its constituent CIQ Interface and IQ Agent, intercepts their private content. That is precisely what the software was installed and designed to do, and plaintiffs' support for this proposition includes statements and a demonstration present in material cited in plaintiffs' complaint. (*See* Sec. II.A, *supra*, at 2-6 (referencing, *inter alia*, interceptions in "real time"); *see also* Sec. IV.B.1.a, *supra*, at n.10 (discussing the interception of text messages before the message is "actually being displayed in the end user's inbox.").) Yet defendants seek to dismiss because the plaintiffs did not use the phrase "contemporaneous with transmission" in their pleadings. The court in *Byrd v. Aaron's, Inc.*, 2014 WL 1327503 (W.D. Pa. Mar. 31, 2014), recently faced a similar request from a defendant and rejected it. (*Id.* at *18 ("Aaron's argues that the allegations regarding their use of the PC Rental Agent to remotely obtain information from the laptops of franchisee customers are insufficient to state a cause of action under the ECPA because Plaintiffs do not allege that this material was obtained while it was in transmission. Perhaps, Aaron's is seeking particular words to follow the statute . . . .").) But as the Court held there, plaintiffs' allegations, which included no particular words re: acquisitions of content simultaneous with its transmittal, were "sufficient to plead an 'intercept' under the ECPA, such that the federal cause of

[10] As Mr. Eckhart illustrates beginning at 12 mins. and 30 secs. into his video, text message content is intercepted while in transit. After showing the process by which the software is intercepting the content on its way to the recipient, he demonstrates further: "Here's where the [text] message is actually being displayed in the end user's inbox. *So all of the IQ Agent's processes is [sic] happening before the end user even sees the SMS*." (*Id.* at 13:20 (emphasis added).)

action survives, regardless of whether Plaintiffs have sufficiently pled that all the material gathered . . . was in transmission.") *Id.* Fortifying the propriety of the court's decision was its recognition of the "sophistication of the technology" in cases such as these, such that it could not be convinced "that there is no plausibility that the collected material was in some state of 'transmission' as envisaged by the statute when it was obtained by [the defendant] . . . ." *Id.* (citing *United States v. Councilman*, 245 F. Supp. 2d 319, 321 (D. Mass. 2003) ("Technology has, to some extent, overtaken language. Traveling the Internet, electronic communications are often—perhaps constantly both 'in transit' and 'in storage' simultaneously, a linguistic but not a technological paradox."), *aff'd*, 373 F.3d 197 (1st Cir. 2004), *rev'd en banc*, 418 F.3d 67 (1st Cir. 2005)); *see also Arrington v. ColorTyme, Inc.*, 972 F. Supp. 2d 733, 747 (W.D. Pa. 2013) (citing and rejecting same complaint from a defendant, and noting "[f]urthermore, given the sophistication of the technology at issue, it is entirely possible that discovery will reveal that the screenshots, keystrokes and pictures were in some state of 'transmission' as envisaged by the statute when they were obtained by PC Rental Agent.").

Only a few days ago Judge Koh rejected a similar request to dismiss, even though in that case, the defendant, Yahoo, argued that the communications there at issue, emails, were "accessed and scanned" after they "*had already reached Yahoo's servers*," such that they were in storage when allegedly intercepted. *See In re Yahoo Mail Litig.*, 2014 WL 3962824, at *6 (N.D. Cal. Aug. 12, 2014) (emphasis in original). But there, the court denied the motion to dismiss because plaintiffs had alleged that emails had been intercepted while they were "in transit." *Id.* at *7. The court held that "[a]t the [motion to dismiss] state, the Court must accept as true Plaintiffs' allegations that the emails were in transit when Yahoo accessed them." *Id.* The court stated that it would "consider Yahoo's argument that the term 'intercept' under the Wiretap Act" did not apply under the circumstances of the case, "if and when Yahoo shows, at the summary judgment stage after discovery, that Yahoo intercepted users' emails after those emails had already reached Yahoo's servers." *Id.* While plaintiffs have not used the phrase "in transit" in their complaint, they respectfully ask for leave to amend to add that phrase to their allegations, should the Court determine it necessary notwithstanding the content of their present allegations. In any event, if defendants wish to challenge whether their interceptions of content actually occurred contemporaneously with the

transmission of such content, a motion to dismiss is not the proper vehicle for doing so. Instead, any such challenge should come after discovery, on a motion for summary judgment or at trial. *See id.*

b. Plaintiffs allege adequately the unlawful acquisition of electronic communications.

Defendants state affirmatively that they do not seek dismissal of plaintiffs' Federal Wiretap Act claims insofar as text message content and URLs incorporating users' search terms are concerned. On the other hand, defendants appear to seek the dismissal of plaintiffs' claims insofar as "the URLs of webpages that an individual has visited . . . even if they contain embedded user ID information" such as a "Facebook ID" are concerned, or even if they "identify the website that directed the user to that URL." (Mot. at 22-23.) Read carefully, defendants do not seek the dismissal of plaintiffs' claims where the content at issue would be user names and passwords entered by a user, for example, a user name and password for a bank account, as distinct from "user ID" carried in an automatically generated HTTP/S referer to another page—the latter of which was at issue in *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1102 (9th Cir. 2014) (when a Facebook user clicked on an ad or icon in Facebook, the web browser would "sen[d] an HTTP request to access the resource identified by the link"; that request "included a referer header that provided both the user's Facebook ID" and the address of the Facebook page "the user was viewing when the user clicked the link"). If anything, insofar as URLs are concerned, defendants seem to seek only dismissal of plaintiffs' claims insofar as they relate to a bare web address (they cite to a case referencing "www.helpfordrunks.com") or to automatically generated identifying information such as that at issue in *Zynga*—so called "record information." *See id.* at 1106-07.

In any event, *Zynga* itself makes plain that, for example, a "Google search URL not only shows that a user is using the Google search engine, but also shows the specific search terms the user had communicated to Google. . . . Under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third-party could amount to disclosure of the contents of a communication." *Id.* at 1108-09 (citation omitted). This sort of use of the Internet is analogous to a PayPal, bank, or Amazon.com customer communicating his or her user name or password to a bank by way of their

being appended to, or a component of, a URL generated by a browser. Plaintiffs have alleged that Carrier IQ Software and its components intercept user names and passwords contained in URLs or HTTP/S strings. (SCAC, ¶¶ 63, 65.) These are contents of electronic communications because a user sends them as messages (please allow me access; here are my credentials) to a website. *See Zynga*, 750 F.3d at 1106 ("Accordingly, we hold that under ECPA, the term 'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication."); *see also In re Google Inc. St. View Elec. Commc'ns Litig.*, 794 F. Supp. 2d 1067, 1071-72, 1082 (N.D. Cal. 2011) (refusing to dismiss claims for violation of the Federal Wiretap Act where "data packets" previously described as containing "whole emails, usernames, passwords and other private data" were "arguably electronic communications," and stating that "Plaintiffs pl[ed] facts sufficient to state a claim for violation of the Wiretap Act."). Accordingly, the Court should not dismiss any claims based on the interception of user names or passwords, or of SMS text message content (or other message content) or Internet search terms.

2. Plaintiffs allege adequately the unlawful use of a device or devices within the meaning of the Federal Wiretap Act.

Throughout their SCAC, plaintiffs allege that defendants used the Carrier IQ Software, including the CIQ Interface and IQ Agent, to intercept their electronic communications. (SCAC, ¶¶ 40-84.) This software is the "device" at issue. *See, e.g., Clements-Jeffrey v. City of Springfield*, 810 F. Supp. 2d 857, 862 (S.D. Ohio 2011) (referring to "certain software," *i.e.*, the device at issue, that allowed defendant "to intercept email and other electronic communications," and refusing to grant summary judgment in defendants' favor on Federal Wiretap Act claim); *In re iPhone App. Litig.*, 844 F. Supp. 2d at 1062 (granting dismissal of Federal Wiretap Act claim, but rejecting alternative basis sought by defendant; claim based on use of iOS 4 *software* to intercept would not have been dismissed on additional statutory exemption ground sought by defendant).

Yet the defendants argue that their software falls outside the statutory definition of device. (Mot. at 23-26.) Citing to a provision of the Federal Wiretap Act that defines what a "device" does not include, 18 U.S.C. § 2510(5)(a), defendants claim that the Carrier IQ Software cannot be a

"device" because it is a component of devices provided to consumers by their wireless carriers in the ordinary course of the carriers' business, and because: (i) the plaintiffs used their phones with this supposed "component" in the ordinary course of plaintiffs' business; and (ii) the carriers used the Carrier IQ Software "component" of plaintiffs' phones in the ordinary course of the carriers' business. (Mot. at 23-24.)

As explained below, this argument fails for several reasons. First, the Carrier IQ Software is not a "component" of plaintiffs' phones. Second, the phones the defendants invoke are the plaintiffs' *own individual phones*—not extension phones, which is what the first subpart of 18 U.S.C. § 2510(5)(a) addresses. Third, plaintiffs' phones—with their Carrier IQ functionality that the carriers disclaim—were not provided to plaintiffs in the ordinary course of the carriers' business. Fourth, the Carrier IQ Software-equipped phones at issue were not being used by the carriers in the ordinary course of their businesses, which means that the second subpart of 18 U.S.C. § 2510(5)(a) does not apply, either. Fifth, the supposed ordinary course of the carriers' businesses is not a matter that can be decided on a motion to dismiss.

Defendants offer no positive case authority for the proposition that their software was a "component" of plaintiffs' devices. (Mot. at 24.) In fact, the dictionary definition of "component" that they offer speaks to a "constituent element, as of a system." (Mot. at 23.) But their software is not a "constituent element" of a phone, like a touchscreen or even an operating system. Their software is in no way elemental to the operation of the phones—to the contrary. Rather, it is simply an attachment that can be removed at will (as Sprint reportedly did). It is like the add-ons in defendants' own authorities. (*See id.* at 24 n.6 (*citing United States v. Murdock*, 63 F.3d 1391, 1395-96 (6th Cir. 1995); *Williams v. Poulos*, 11 F.3d 271, 280 (1st Cir. 1993); *Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 740 (4th Cir. 1994)).) Because their software is not a "component" of plaintiffs' devices, defendants' argument fails at the outset.

Next, defendants, in invoking the first subpart of 18 U.S.C. § 2510(5)(a), are attempting to invoke the extension exception to the law. (Mot. at 23-25.) That is an exemption that Congress built into the law for extension phones in a given location, so that listening in on a call on a second phone in one's own place (if done in the ordinary course of business) would not be deemed an interception.

See, e.g., Briggs v. American Air Filter Co., 630 F.2d 414, 418 (5th Cir. 1980) (setting forth history of the exemption and stating that "[w]hen the bill was passed, the blanket exception for extension phones provided by communications common carriers in the ordinary course of their business was limited to such phones when they were being used in the ordinary course of the subscriber's or user's business"); *Babb v. Eagleton*, 616 F. Supp. 2d 1195, (N.D. Okla. 2007) ("Title III [referring in heading to 18 U.S.C. § 2510(5)(a)(i)] contains what has been referred to by other courts as an 'extension phone exemption' . . . or 'an exemption for business use of a telephone extension'") (citations omitted). Here, defendants are referring to plaintiffs' own devices, not extensions. So their contention under the first subpart of 18 U.S.C. § 2510(5) fails.

Moreover, the focus here is on the Carrier IQ Software—that is what defendants assert is the "component" here at issue. (Mot. at 24.) Even if an extension phone were at issue here, rather than plaintiffs' own devices, defendants cannot demonstrate that the carriers would consider supplying phones to consumers that intercept their text messages, Internet search terms, and user names and passwords as a practice in the ordinary course of the carriers' business (and that at least sometimes transmit their private content to third-parties such as Google or HTC). After all, Sprint and AT&T both advised Sen. Franken that they did *not* seek to collect text messages or Internet search terms. (Newby Decl. Ex. 2 at 3 and Ex. 1 at 2-4.) (Defendants' claim that Sprint intended to collect URLs is misleading because URLs need not contain Internet search terms, user names, or passwords. In its letter to Sen. Franken, Sprint specifically disclaimed any collection of search terms. (*Id.* Ex. 2 at 3.))

As for the second subpart of 18 U.S.C. § 2510(5)(a), defendants cannot demonstrate that the Carrier IQ Software placed on plaintiffs' phones was used by the carriers in the ordinary course of the carriers' businesses. (Mot. at 25-26.) The software, especially given its unlawful and carrier-disclaimed functionalities, cannot be said to be instrumental to the provision of services by the carriers; the interception of contents of customers' private electronic communications as alleged by the plaintiffs were not part of the carriers' business plans. *See In re: Google Inc. Gmail Litig.*, 2014 WL 5423918, at *11 (N.D. Cal. Sept. 26, 2013) ("In light of the statutory text, case law, statutory scheme, and legislative history concerning the ordinary course of business exception, the Court finds that the section 2510(5)(a)(ii) exception is narrow and designed only to protect electronic

communications service providers against a finding of liability under the Wiretap Act where the interception facilitated or was incidental to the provision of the electronic communication service at issue."); *Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 505 (2d Cir. 2005) (at issue were emails received and stored by the defendant even after addressee closed its account; defendant presented testimony that it routinely continued to receive and store emails after an account was canceled, and that it "did not have the ability to bounce e-mail back to senders after termination of an account"; thus, the alleged interceptions were deemed a necessary part of its ability to provide email services). This lack of an instrumental tie to the provision of cellular telephone service is doubly so with respect to plaintiffs' allegations of interception over private Wi-Fi, rather than the carriers' networks.

Finally, as *Hall*, with its reference to testimony, and the follow-on decision in the *Google Gmail Litig.* makes plain, whether the software was used in the ordinary course of the non-party carrier businesses cannot properly be resolved on a motion to dismiss. *See In re: Google Inc. Gmail Litig.*, 2014 WL 294441, at *3 n.2 (N.D. Cal. Jan 27, 2014) ("[T]he Court finds that factual development would be necessary in determining whether Google's interceptions fall within the 'ordinary course of business' exception."); *see also id.* at *1-2 (citing to E.D. Tex. decision in *Dunbar v. Google, Inc.*, in which that Court had "rejected Google's 'ordinary course of business' argument" and held "'the applicability of the "ordinary course of business exception" . . . cannot be resolved at the pleading stage.'") (internal citation omitted). Indeed, after discovery, plaintiffs will probably be able to demonstrate that the interceptions complained of violate Google's internal policies, *see id.* at *3 n.2, such that they cannot be considered incidents of the carriers' ordinary course of business.

3. Plaintiffs allege adequately intentional interceptions by the manufacturer defendants.

The manufacturer defendants further argue that they cannot have intercepted plaintiffs' content because there supposedly was no "acquisition" by them of that material. (Mot. at 26-28.) The manufacturers contend that the plaintiffs do not even allege any such acquisition. But "acquisition" is part of the definition of "intercept" under the Federal Wiretap Act, 18 U.S.C. § 2510(4), and plaintiffs allege interception by the manufacturers throughout the SCAC, including by

way of the CIQ Interface that HTC and likely all other manufacturers wrote and installed.[11] (*See* SCAC, ¶¶ 62-63; CIQ White Paper at 6.) Where the manufacturers' alleged direct liability is concerned, it is noteworthy that one of the two cases cited by the defendants, *Kirch v. Embarq Mgmt. Co.*, 2011 WL 3651359 (D. Kan. Aug. 19, 2011), was decided on summary judgment, and the other, *Bohach v. Reno*, 932 F. Supp. 1232 (D. Nev. 1996), was a preliminary injunction case. Neither of them employed the deferential standard applicable in deciding a motion to dismiss.

Moreover, neither decision applies the binding definition of "acquisition" set forth by the Ninth Circuit. The manufacturers argue that if a "defendant itself did not acquire any data obtained by [a] device," then the defendant "does not engage in interception." For this proposition they rely on *Kirch*, 2011 WL 3651359, at *4, a District of Kansas case. They also cite to *Bohach*, 932 F. Supp. at 1236, to support their contention that "passing data on without storing or recording its contents does not constitute an 'interception.'" (Mot. at 27.) But neither case aids the defendants in light of the Ninth Circuit's decision in *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009). As the court held there: "The Wiretap Act defines 'intercept' as 'the aural or other acquisition of the contents of any wire . . . communication [the provision also includes electronic communications] through the use of any electronic, mechanical, or other device.' 18 U.S.C. § 2510(4). *Such acquisition occurs 'when the contents of a wire communication are captured or redirected in any way.'*" *Noel*, 568 F.3d at 749 (citing *Rodriguez*, 968 F.2d at 136 (emphasis added)).

It was the manufacturers' actions, by way of installing working Carrier IQ Software, that caused the acquisition, *i.e.*, the "captur[ing] or redirec[ion]," of plaintiffs' content. (SCAC, ¶¶ 61, 63, 77.) *They* intercepted the plaintiffs' text messages and Internet search terms, among other material, by way of software they wrote and placed on phones directed to consumers. Further, while the manufacturers point to the carriers as recipients of the content by way of transmittals, Mot. at 26, the Ninth Circuit stated that "[n]o new interception occurs when a person listens to or copies the

[11] The manufacturers pretend that they merely installed someone else's product and were done with it. But as plaintiffs allege, the manufacturers knew exactly what the Carrier IQ Software was designed to intercept because they wrote and installed the CIQ Interface that captured and redirected, *i.e.*, intercepted, plaintiffs' private content. (*See* SCAC, ¶¶ 61, 63, 77.) Each also installed the IQ Agent. Under the defendants' own preferred definition of "intentional," they intended interceptions because it was their "conscious objective" in writing and installing the CIQ Interface, and the IQ Agent as well, to intercept the material at issue. (*See* Mot. at 28-29 (citing to legislative history regarding the meaning of "intentional").)

communication that has already been captured or redirected." *Noel*, 568 F.3d at 749. Thus, insofar as the interceptions at issue occurred—and plaintiffs allege that they did—the manufacturers and Carrier IQ were the culpable actors under the law.

Two final points bear noting. First, Carrier IQ has stated that some manufacturers were also its customers. (SCAC, ¶ 68.) Discovery will reveal which manufacturers were customers, and precisely what data or content they received. Second, the manufacturers argue that plaintiffs "at best" claim aider-and-abettor liability on their part, and that such liability is not available under the Federal Wiretap Act. (Mot. at 28 n.8.) But their own cited Ninth Circuit authority for this statement, *Freeman v. DirecTV, Inc.*, 457 F.3d 1001 (9th Cir. 2006), in fact leaves the door open for that sort of liability. *See id.* at 1008-09 (pointing out that the Tenth Circuit may have meant in *Quigley v. Rosenthal*, 327 F.3d 1044 (10th Cir. 2003), to allow for conspiracy claims under 18 U.S.C. § 2511, and noting that Section 2511 is broader than the other provisions before it; as the court noted, "Section 2511 imposes liability on 'any person' and then lists a number of prohibited actions."). 18 U.S.C. § 2511(1)(a) is indeed broad enough to encompass aider-and-abettor or conspiracy liability, and as defendants acknowledge, plaintiffs' allegations are broad enough to encompass it. For this reason, too, plaintiffs' claims under the Federal Wiretap Act should not be dismissed.

C. Plaintiffs' state privacy act claims are properly pled.

1. Plaintiffs are entitled to relief under the individual states' privacy acts.

Plaintiffs bring claims on behalf of themselves and other similarly situated individuals under Cal. Penal Code § 502 and the privacy acts of 35 other states. The state statutes are modeled after the Federal Wiretap Act and protect the same type of conduct that is the subject of Count I, namely, the intentional interception of communications. (SCAC, ¶ 113(a)-(hh).) Count II, Violation of State Privacy Acts, incorporates by reference every allegation that precedes it as if it were set forth therein, and therefore adequately states a claim under the referenced states' laws. (SCAC, ¶ 100.)

Plaintiffs are entitled to relief under the state statutes because the defendants intentionally intercepted plaintiffs' communications. (*See* SCAC, ¶¶ 61, 63, 65-72 (discussing the extent of Carrier IQ's interception of communication); *see also* SCAC, ¶ 69 (noting the serious consequences of Carrier IQ's interception of "personal, private, confidential, and sensitive data" and the "grave

breaches of privacy").) The Carrier IQ Software and Interface were intentionally "designed, authored, programmed and installed" by defendants to surreptitiously receive and intercept data. (SCAC, ¶¶ 61-63.) These data intercepted by defendants constitute communications as defined by each state's statute(s). (*See, e.g.*, SCAC, ¶¶ 68, 70, 72, 81 (exchange of SMS text message content); SCAC, ¶¶ 65, 71-73, 121 (unencrypted HTTP web queries); *id.*, ¶¶ 1, 40, 46, 49, 65, 72 (noting other keystrokes; in-coming and out-going telephone numbers; granular geo-location information; application purchase and use data; and other information that has been sent to the device, system, or logcat logs captured by Carrier IQ).) Defendants argue that the analysis of the federal claim obviates any need to parse the state statutes. However, this argument contradicts the established notion that Congress' drafting of the Federal Wiretap Act was not an attempt to occupy the field of privacy, but was merely an attempt to establish minimum standards. *Leong v. Carrier IQ, Inc.*, 2012 U.S. Dist. LEXIS 59480 (C.D. Cal. Apr. 27, 2012) (citing *People v. Conklin*, 12 Cal. 3d 259, 271 (1974)). Therefore, analysis limited to federal law interpretation is insufficient to determine whether a state claim survives.

In fact, many states' statutes are more protective than the Federal Wiretap Act. *See Leong*, at *10-13 (citing *Conklin*, 12 Cal. 3d at 273) (California)[12]; (Connecticut) *State v. Grant*, 404 A.2d 873, 877-78, n.3 (Conn. 1978) (the Connecticut wiretap and electronic surveillance statutes are "in many respects more stringent than the equivalent federal act."); (Florida) *State v. Tsavaris*, 394 So. 2d 418, 422 (Fla. 1981) (noting that the Florida statute "evinces a greater concern for the protection of one's privacy interests in a conversation than does the Federal Wiretap Act" and stating that Florida does have a two-party consent rule); (Iowa) *State v. Spencer*, 737 N.W.2d 124, 130 (Iowa 2007) (citing *Davenport v. Pub. Emp't Relations Bd.*, 264 N.W.2d 307, 313 (Iowa 1978)) (interpretations of the

[12] Defendants half-heartedly argue that California's Invasion of Privacy Act does not prevent their interception of private communications because plaintiffs have not alleged interception between two devices. (Mot. at 3 n.10.) Cal. Penal Code § 632.7(a) prohibits the interception of "a communication transmitted between two cellular radio telephones, a cellular radio telephone and landline telephone, two cordless telephones, a cordless telephone and a landline telephone, or a cordless telephone and a cellular radio telephone." Here, plaintiffs have alleged that defendants intercepted SMS text messages, intercepted communications between cellular telephones and a server which communicates back to the phone with requested information, and intercepted geo-location queries. (SCAC, ¶¶ 1, 2, 46, 63, 65, 102, 105.) These are cellular phone activities that occur between two communication devices as contemplated by the statute. To the extent that defendants are arguing that plaintiffs have not adequately alleged an "interception" during the flight of the communication, this issue is addressed in Sec. C.1 of this memorandum.

[Federal Wiretap Act] are "neither conclusive nor compulsory" on the Iowa statute); (Maryland) *In re Info. Mgmt. Servs., Inc. Derivative Litig.*, 81 A.3d 278, 294 (Del. Ch. 2013)[13] (Maryland Wiretap Act "has imposed stricter requirements for civilian monitoring than has federal law," since an "interception" will be lawful only if all the participants to the communication give their consent to interception). Therefore, dismissal of the state claims based on any deficiency in the federal allegations would be improper.

2. Plaintiffs' references to "endeavoring to intercept" are proper as certain states proscribe that activity by statute.

Defendants also challenge plaintiffs' references to "endeavoring to intercept" for states that do not provide for such a claim by statute. (Mot. at 32 n.11.) However, in certain states, "endeavoring to intercept" is, in fact, a violation of the statute.[14] Pursuant to a plain reading of the SCAC, plaintiffs seek damages to the full extent allowable under each states' applicable civil remedy statute for violation of that states' privacy statute. (SCAC, ¶113(a)-(hh).) Therefore, defendants' challenge to such allegations are without merit.

3. Plaintiff Sandstrom's claim under the Washington Privacy Act is adequately pled.

a. Plaintiff Sandstrom has sufficiently pled an "intentional interception" under the Washington Privacy Act.

Plaintiff Sandstrom has sufficiently pled an "intentional interception," and defendants' reliance on *State v. Roden*, 321 P.3d 1183 (Wash. 2014) to argue otherwise (Mot. at 32:15-33:3) is misplaced. (*See* SCAC, ¶¶ 1, 2, 40, 46, 61-65, 67.) In fact, *Roden* recognizes that Washington's Privacy Act broadly protects individuals' privacy rights and is one of the most restrictive electronic

[13] Defendants' citation to *In re Info. Mgmt. Servs.*, 81 A.3d at 294, Mot. at 32:6-7, is inaccurate. First, the court was deciding a motion to compel, not a motion to dismiss. Second, the court's analysis did not discuss the plaintiffs' allegation of "contemporaneous interception," but turned on the issue of consent to the interception. *Id.*

[14] Fla. Stat. § 934.03 (proscribing intentional interception, *endeavoring to intercept*, and *procuring another* person to intercept, electronic communication) (emphasis added); Iowa Code § 808B.2(1)(a)-(d) (proscribing "*endeavors to intercept*," "*endeavors to use*," and "*endeavors to disclose*") (emphasis added); Md. Courts & Jud. Pro. Code § 10-402(a)(1)-(3) (proscribing "*endeavoring to intercept*," "*endeavoring to disclose*" and "*endeavoring to use*") (emphasis added); N.H. Rev. Stat. § 570-A:2, I(a)-(d) (proscribing "*endeavors to intercept*," "*endeavors to use*," and "*endeavors to disclose*") (emphasis added); Tex. Penal Code § 16.02 (b) (providing "A person commits an offense if the person: (1) intentionally intercepts, *endeavors to intercept*, or procures another person to intercept…(2) intentionally discloses or *endeavors to disclose*…(3) intentionally uses or *endeavors to use*…(5) intentionally uses, *endeavors to use*, or *procures any other person* to use…") (emphasis added); Wis. Stat. § 968.31(1)(a)-(d) (proscribing "*attempts to intercept*," "*attempts to use*" and "*attempts to disclose*") (emphasis added).

surveillance laws ever promulgated in that it "significantly expands the minimum standards of the federal statute…and offers a greater degree of protection to Washington citizens." *Roden*, 321 P.3d at 1185-86.

Defendants not only misinterpret *Roden*, but also cite it in an attempt to limit the Washington Privacy Act to a discrete factual scenario that the statute simply does not envision. (Mot. at 32:15-33:3.) In *Roden*, an officer opened, read, and responded to text messages sent to a suspect. The question was whether the officer's active participation in the sending of the messages defeated the communications from being "intercepted" within the meaning of the Act. Since the Washington statute does not define the term "intercept," the court gave the term its ordinary meaning, "to stop… before arrival… or interrupt the progress or course." *Roden*, 321 P.3d at 1188. The court held that the activities of the officer easily met this definition since he affirmatively manipulated the suspect's phone and responded to text messages before the suspect was able to view them. *Id.* at 1189. That said, the court did not limit the Washington Privacy Act to this discrete factual scenario. In fact, as the court in *Roden* explained, sending a text message is much like mailing a letter, and "the ordinary meaning of 'intercept' encompass[es] opening and reading a letter in someone else's mailbox before they receive it." *Roden*, 321 P.3d at 1189. This example makes clear that plaintiff Sandstrom need not show "that the Carrier IQ Software interrupted any communications or stopped them from reaching him or the recipient to who he directed them" in order to sufficiently allege interception as Defendants argue. (Mot. at 33:3-5.) The *Roden* court's letter analogy demonstrates that an interception is made once a party intentionally receives the communication meant for another. This reasoning is bolstered by the fact that, as defendants acknowledge, the Washington Privacy Act does not distinguish between communications that are in electronic storage and those that are not. *Roden*, 321 P.3d at 1189; Mot. at 33:7-8. Even if the communication is stored on a device before it is intercepted, the interception is a violation of the statute. As such, plaintiffs have sufficiently pled an intentional interception pursuant to the Washington Privacy Act.

b. The Washington Privacy Act protects the communications at issue in this case.

Defendants also argue that the Washington statute does not provide plaintiff Sandstrom relief

for the interception of any data other than text messages. (Mot. at 33:11-19.) Again, defendants' claims are misguided. In *State v. Gunwall*, 720 P.2d 808, 816 (Wash. 1986), the court broadened the scope of the Washington Privacy Act and extended the definition of a "private communication transmitted by telephone" to include data intercepted by a pen register, a device that attaches to telephone lines to identify all the phone numbers dialed, regardless of whether the call is completed. *Id*. at 813. The court found that even if a call failed to go through and no other person was made a party to the transmission, the data captured by the pen register still came within the definition of a "private communication transmitted by telephone" despite not necessarily being "between the two [or more individuals.]" *Id*. at 813.[15]

Defendants rely on *Cousineau v. Microsoft Corp.*, 2012 U.S. Dist. LEXIS 189347, at *32 (W.D. Wash. June 22, 2012), but the holding in *Cousineau* is limited as that case exclusively discussed the surreptitious interception of the plaintiff's geo-location data through her use of the camera application. *Id*. at *3-4. The court considered whether the plaintiff was communicating when she used her camera and her geo-location data was intercepted. *Id.* at *31. The court concluded that without an individual on the other end of her communication, the transmission of the plaintiff's geo-location data could not be considered a communication under the Washington Act. *Id*.

Here, defendants intercepted plaintiff Sandstrom's communications sent to, and intended only for, another party—specifically, the internet servers, search engines, geo-location applications, and other internet entities like Google and PayPal. (SCAC, ¶ 46.) Further unlike the plaintiff in *Cousineau*, plaintiff Sandstrom intended these communications to be transmitted to that other party with the goal of receiving responses. These search queries, passwords, and geo-location information often constituted or included sensitive, private information. Therefore, the data allegedly intercepted by defendants qualifies as communications under the Washington Act. (SCAC, ¶¶ 1, 61-63, 65, 67.)

[15] Here, the Carrier IQ Software not only collects keystroke data in the same fashion as a pen register, but also collects a broader scope of communication. (SCAC, ¶¶ 1, 46, 65, 102.)

4. Plaintiff Szulczewski has a viable claim under the Illinois Eavesdropping Statute.

Although 720 Ill. Comp. Stat. 5/14-2(a)(1) and (3) of the Illinois Eavesdropping Statute have been declared facially unconstitutional,[16] that is not fatal as plaintiff Szulczewski still has a claim under the remaining section of Ill. Comp. Stat. 5/14-2(a)(2). As quoted in paragraph 113(g) of the SCAC, this section provides in pertinent part:

> (a) A person commits eavesdropping when he:
>
> (2) Manufactures, assembles, distributes, or possesses any electronic, mechanical, eavesdropping, or other device knowing that or having reason to know that the design of the device renders it primarily useful for the purpose of the surreptitious hearing or recording of oral conversations or the interception, retention, or transcription of electronic communications and the intended or actual use of the device is contrary to the provisions of this Article; . . .

Such activities have been alleged.

Defendants designed, authored, programmed, and installed the Carrier IQ Software which purposefully enabled the consumers' mobile devices to surreptitiously record, intercept, retain, or transcribe electronic communication, content and personal, private, and sensitive data. (SCAC, ¶¶ 61-63, 67, 80.) Therefore, the facts pled by plaintiff Szulczewski are sufficient to establish an eavesdropping claim under Section 5/14-2(a)(2), as alleged in the SCAC. (*See* SCAC, ¶¶ 51, 57, 61-67.) Because Carrier IQ and the OEMs have committed eavesdropping by manufacturing and distributing the Carrier IQ Software, which was designed for the primary purpose of the surreptitious interception, retention, and transcription of electronic communication in contravention of the provisions of Article 14 of the Illinois Statutes, defendants' motion to dismiss should be denied. *See* Ill. Comp. Stat. 5/14-2(a)(2).

5. The Michigan Eavesdropping Statute protects against the invasive intrusion of privacy perpetrated by defendants.

Defendants seek to dismiss plaintiff Cline's claims related to electronic communication. (Mot. at 34:2-18.) As cited in paragraph 113(g) of the SCAC, the Michigan Eavesdropping Statute, Mich. Stat. § 750.539c, prohibits "eavesdrop[ping] on [a] conversation without the consent of all

[16] *See People v. Clark*, 6 N.E.3d 154 (Ill. 2014) (finding unconstitutional recording provision of Illinois Eavesdropping Statute, 720 Ill. Comp. Stat. 5/14-2(a)(1)(A)); *People v. Melongo*, 6 N.E.3d 120 (Ill. 2014) (holding unconstitutional recording provision, 720 Ill. Comp. Stat. 5/14-2(a)(1), and publishing provision, 720 Ill. Comp. Stat. 5/14-2(a)(3), of Illinois Eavesdropping Statute).

parties thereto." Mich. Stat. § 750.539a(2) defines eavesdropping as "to overhear, record, amplify or transmit any part of the private discourse of others." Contrary to defendants' assertion, courts have recognized the term "discourse" within the meaning of the Michigan Eavesdropping Statute as "the private, oral, or written communication of others." *Lewis v. LeGrow*, 670 N.W.2d 675, 683 (Mich. App. 2003). As alleged in the SCAC, plaintiff Cline's claims relate to electronic communication. (*See, e.g.*, SCAC, ¶¶ 68, 70, 72, 81 (exchange of SMS text message content); *id.*, ¶¶ 65, 71-73, 121 (unencrypted HTTP web queries); *id.*, ¶¶ 1, 40, 46, 49, 65, 72.) Plaintiff Cline's allegations concern the recordation and transmission of written textual communication without consent (SCAC, ¶¶ 1, 24, 40, 49, 51, 70, 77, and 79), and claims related to electronic communication are protected as written communication. Plaintiff Cline's claims are well pled under the Michigan Eavesdropping Statute.

Defendants rely on *Bailey v. Bailey*, 2008 U.S. Dist. LEXIS 8565, at *18 (E.D. Mich. Feb. 6, 2008), to argue that use of software which records the keys pushed on a computer does not violate the Michigan Eavesdropping Statute as the statute purportedly requires an "oral exchange of sentiments." (*See* Mot. at 34:19-27, 35:4-7.) This argument fails because in *Bailey*, the court's analysis hinged on whether the plaintiff was engaged in a "conversation." *Id.* at *20. There, the key logging software was "designed to record every keystroke made on the computer and store it in a text file on the computer's hard drive." *Id.* at *3. The software permitted the defendant to learn plaintiff's passwords, which were then used by the defendant to access the plaintiff's email and private message system. *Id.* at *3-4. The court reasoned that the Michigan Eavesdropping Statute did not apply as the key logger software only recorded the plaintiff's side of the conversation. *Id.* at *20-21.

In contrast here, the Carrier IQ Software "intercept[s] communications and a significant amount of data and content, *including* keystrokes." (SCAC, ¶ 46 (emphasis added).) Similar to oral discussions or the exchange of letters, text messages are conversational, and often include private, confidential, and personal matters communicated to another person or server. (*See, e.g.*, SCAC, ¶¶ 8-25.) Additionally, the written communications captured by the Carrier IQ Software fit within the requirements of a "private communication" within the meaning of MCLS § 750.539c because plaintiff had a reasonable expectation that access to the sensitive communication transmitted from

his cellular device would be limited to the specified recipients of the information. *See People v. Stone*, 621 N.W.2d 702, 704-05 (Mich. 2001) (construing "private conversation" within the Michigan Eavesdropping Statute as "a conversation that a person reasonably expects to be free from casual or hostile intrusion or surveillance"). Accordingly, defendants' motion should be denied.

6. Plaintiffs have adequately pled a claim under the California Comprehensive Data and Fraud Act.

As set forth in Section IV.A above, plaintiffs have Article III standing and have alleged a cognizable "damage or loss" caused by Carrier IQ.

7. Plaintiffs have properly alleged defendants' violation of the CCDAFA.

The SCAC alleges that defendants violated Cal. Penal Code § 502 by knowingly accessing, copying, using, making use of, interfering, and/or altering plaintiffs' and prospective class members' data such as URLs containing HTTP and HTTPS query strings embedded with information including search terms, user names, passwords, and granular geo-location information; granular geo-location information apart from that transmitted in URLs; text messages; telephone numbers dialed and received; other keystrokes; and application purchases and uses. (SCAC, ¶ 105.[17]) These allegations, which borrow from the statutory language found in Cal. Penal Code § 502 (c)(1)-(9), are supported by all facts alleged in the SCAC at paragraphs 40-85, which describe the manner in which the Carrier IQ Software and the CIQ Interface were surreptitiously pre-loaded in plaintiffs' cell phone devices to purposefully access, use, and interfere with plaintiffs' data without plaintiffs' consent. *See Craigslist*, 2009 U.S. Dist. LEXIS 132433, at *34 (holding plaintiff sufficiently stated claim under Section 502(c) when it alleged that defendant knowingly accessed its computers and computer system and without authorization, copied and made use of plaintiff's data). Therefore, plaintiffs have complied with Rule 9(b)'s pleading requirements.

[17] Although claims for violations of CCDAFA are subject to Federal Rule 9(b)'s heightened pleading requirement, *Vess*, 317 F.3d at 1103-04, the Ninth Circuit has ruled that when facts concerning fraud are within the opposing party's knowledge, the heightened pleading standard may be relaxed. *Craigslist, Inc. v. Mesiab*, 2009 U.S. Dist. LEXIS 132433, at *34 (N.D. Cal. Sept. 14, 2009) (citing *Moore v. Kayport Package Express*, 885 F.2d 531, 540 (9th Cir. 1989)). Although a large amount of the facts concerning defendants' unlawful interference with plaintiffs' mobile devices are unknown to plaintiffs, the SCAC more than adequately alleges a violation under CCDAFA. The cases cited by defendants do not require claims under Cal. Penal Code § 502 to be pled in any special manner.

8. Plaintiffs have properly alleged that defendants acted "without permission" under the California Penal Code.

Cal. Penal Code § 502 prohibits access to plaintiffs' devices without permission. Courts in this district have held that "without permission" requires that a defendant access a network without consent and in a manner that circumvents technical or code based barriers in place to restrict or bar a user's access. *Perkins v. LinkedIn Corp.*, 2014 U.S. Dist. LEXIS 81042, at *60 (N.D. Cal. June 12, 2014) (citing *In re iPhone Application Litig.*, U.S. Dist. LEXIS 106865 (N.D. Cal. Sept. 20, 2011); *In re Google Android Consumer Privacy Litig.*, 2013 U.S. Dist. LEXIS 42724 (N.D. Cal. Mar. 26, 2013)).

Defendants argue that plaintiffs have not alleged that defendants breached any technical or code-based barrier. In this regard, defendants' reliance on *Perkins*, *supra*, is unavailing. In *Perkins*, the plaintiffs alleged that once they provided LinkedIn with their email address, LinkedIn used an open connection to the email service to download a user's password, instead of requiring the user to re-enter their password. The *Perkins* decision is distinguishable in many ways. First, plaintiffs authorized LinkedIn to access their contacts by affirmatively consenting to the access. *Perkins*, 2014 U.S. Dist. LEXIS 81042, at *46. In addition, LinkedIn merely skipped the step of requiring users to input their passwords when the user had their email open in another tab or had not logged out of their email account. Ultimately, the plaintiffs in *Perkins* had consented to provide LinkedIn with their email password and there was no reason to believe that they would not ultimately do so. *Id.* at *64.

In contrast, plaintiffs' SCAC adequately alleges that defendants acted without permission by circumventing technical and code based barriers to restrict defendants' access. First, the Carrier IQ Software intercepts outgoing web queries and search terms sent via the HTTPS protocol. (SCAC, ¶¶ 46, 47, 65, 71-73, 121.) These queries should be encrypted, but defendants recorded this content in unencrypted, human-readable form. (SCAC, ¶¶ 1 n.2, 46, 71, 77 (discussing the security capabilities of the HTTPS protocol and alleging Carrier IQ evasion of the added level of security).) Therefore, defendants have circumvented the code based barriers of the HTTPS in order to log data in human-readable form. Second, although users are able to delete other applications running on their devices, defendants manipulated the software to prevent Carrier IQ from being deleted,

therefore manipulating the technical barriers of access. (SCAC, ¶¶ 41, 64.) Third, GPS-based geo-location information is typically only accessible when a device is on a mobile carrier's cellular network. However, Carrier IQ manipulated the technical barrier to make GPS-based geo-location information accessible even when a search is conducted over Wi-Fi. (SCAC, ¶ 65.) Fourth, SMS text messages traditionally use standardized communications protocols to exchange short text messages over cellular data networks. (SCAC, ¶ 46.) However, Carrier IQ manipulated the technical and code based barriers of the device to intercept SMS content when a phone was used solely over Wi-Fi. (SCAC, ¶¶ 46, 77, 80.) In addition, the SMS content is logged in unencrypted, human-readable form by Carrier IQ instead of in communications protocols. (SCAC, ¶ 46.) Therefore, because the SCAC is replete with facts to establish defendants' acquisition of data through bypass of technical and code based barriers, plaintiffs have adequately alleged a claim under the CCDAFA.

D. Plaintiffs' consumer protection claims have been pled with sufficient specificity.

1. Plaintiffs have pled a claim under California's Unfair Competition Law in sufficient detail to enable defendants to respond.

To state a claim under California's unfair competition law ("UCL"), plaintiffs must allege an "unlawful, unfair, or fraudulent business act or practice." Cal. Bus. & Prof. Code § 17200. Because Section 17200 is written in the disjunctive, it establishes three varieties of unfair competition—acts or practices which are unlawful, or unfair, or fraudulent. *Id*. at 1102. Therefore, plaintiffs' 17200 claim under each of these three prongs must be evaluated individually, as each of those three adjectives captures "a separate and distinct theory of liability." *Rubio v. Capital One Bank*, 613 F.3d 1195, 1293 (9th Cir. 2010). Sections 17200's coverage has been described as "sweeping," and its standard for wrongful business conduct is "intentionally broad." *In re First Alliance Mortg. Co.*, 471 F.3d 977, 995 (9th Cir. 2006). As shown below, plaintiffs have pled sufficient facts to state a claim under Section 17200.

a. Plaintiffs have adequately alleged that defendants' conduct was unlawful.

The unlawful prong of the UCL prohibits "anything that can properly be called a business practice and that at the same time is forbidden by law." *Cel-Tech Commc'ns, Inc. v. L.A. Cellular*

Tel. Co., 20 Cal. 4th 163, 180 (1999). Virtually any state, federal, or local law can serve as the predicate for an action under Section 17200. *Id.* at 1102-03. Here, plaintiffs allege that defendants' business acts and practices are unlawful because they violated the Federal Wiretap Act and Cal. Penal Code §§ 502 and 632.7. (SCAC, ¶ 118.) Additionally, plaintiffs allege that HTC's conduct with respect to the logging issue described in the SCAC, per the FTC's Complaint and Final Decision and Order, violated the FTC Act, such that those business acts and practices also violated the UCL. *Id.*[18]

Defendants nevertheless argue that plaintiffs' allegations are (1) not sufficient to state those predicate claims and (2) not plead with particularity as to how the facts of this case pertain to those statutes and how defendants violated them. (Mot. at 39:16-40:13.) That is not the case, as discussed in Sections IV.B and IV.C above. Moreover, the FTC's investigation of HTC resulted in findings that HTC's practices injured consumers and was an unfair practice. (SCAC, ¶¶ 75-82.) These detailed allegations, including the FTC's findings, are more than adequate to plead a claim under the unlawful prong of the UCL. *Id.*

b. Plaintiffs have adequately alleged that defendants' conduct was unfair.

The UCL also creates a cause of action for a business practice that is "unfair" even if not specifically proscribed by other laws. *Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1143 (2003). An unfair business practice occurs, within the meaning of the UCL, when it offends an established public policy or when the practice is immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers. *Spiegler v. Home Depot U.S.A., Inc.*, 552 F. Supp. 2d 1036, 1045 (C.D. Cal. 2008). As noted in *In re iPhone Litig.*, *supra*, 844 F. Supp. 2d at 1073-74, in consumer cases, the question of what constitutes an unfair business practice is somewhat unsettled:

> Some appellate state courts have applied the balancing test under *S. Bay Chevrolet v. Gen. Motors Acceptance Corp.*, 72 Cal. App.4th 861, 886–87, 85 Cal.Rptr.2d 301 (1999), which requires the Court to "weigh the utility of the defendant's conduct

[18] Because reliance is not an element of the predicate violations, plaintiffs do not need to show reliance on any misrepresentations by defendants to plead a claim under the "unlawful" or "unfair" prongs of 17200. *See Kane v. Chobani, Inc.*, 973 F. Supp. 2d 1120, 1130 (N.D. Cal. 2014) (holding that there is a reliance element for claims brought under the UCL to the extent the predicate unlawful conduct is based on misrepresentations).

> against the gravity of the harm to the alleged victim." *See McKell*, 142 Cal. App.4th at 1473, 49 Cal.Rptr.3d 227. Others have required a plaintiff to show that a practice violates public policy as declared by "specific constitutional, statutory or regulatory provisions" or that the practice is "immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers." *Bardin v. DaimlerChrysler Corp.*, 136 Cal. App.4th 1255, 1260–61, 1268, 39 Cal.Rptr.3d 634 (2006); *see also Lozano*, 504 F.3d at 736; *Rubio v. Capital One Bank*, 613 F.3d 1195, 1204–05 (9th Cir.2010) (assessing plaintiff's UCL claim for unfair conduct under only the first two tests).

Id. at 1073. Regardless of what test was applied, the court concluded that allegations regarding defendants' collection and dissemination of personal information without the knowledge or consent of mobile device users were sufficient to state a claim under the unfair prong of 17200. *Id*.

The same analysis applies here where plaintiffs have alleged that defendants' acts and practices were unfair under the UCL, given that plaintiffs have been misled regarding the nature and integrity of defendants' goods and services, and that they suffered injury regarding the privacy and confidentiality of their personal information and the use of their devices' resources. (SCAC, ¶ 119.) Plaintiffs further allege that the defendants conduct is unfair because it offends California public policy as reflected in the right to privacy enshrined in the state constitution; Cal. Penal Code §§ 502, 631, and 632,7; and, California statutes recognizing the need for consumers to safeguard their privacy interests, including Cal. Civ. Code § 1798.80. *Id*.[19] Plaintiffs also allege that defendants' acts and business practices were unfair because defendants knew that consumers care deeply about personal, private, confidential, and sensitive information, yet they hid software on their mobile devices that intercepted that data and transmitted most of it off their devices. *Id*. As in *In re iPhone Litigation*, under either test, this conduct cannot be said to be insufficient as a matter of law to state a claim under the unfair prong of 17200.[20]

The detailed information in plaintiffs' complaint is sufficient to support a finding of unfairness in that the subject conduct violated public policy, *i.e.*, the right to privacy declared by

[19] Plaintiffs have explained in detail why the acts of defendants run afoul of plaintiffs' privacy rights enshrined in the state constitution and California statutes. (*See* SCAC, ¶ 119; *see also id*., ¶¶ 47, 49, 61-74; 75-82, 83-85.)

[20] As stated above, plaintiffs have stated a claim for violations of Cal. Penal Code §§ 502 and 632.7. (*See* Secs. IV.C.1. and IV.C.8 above.) Thus, defendants' argument that this claim must fail because the predicate violations have not been adequately pled should be rejected. Moreover, as noted above, the "unfair" prong does not require that the conduct be proscribed by other laws. Defendants' argument, therefore, conflates the requirements of the "unlawful" and the "unfair" prongs of the UCL.

those statutes and the state constitution, and/or that the conduct was immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers. *In re iPhone Litig.*, 844 F.Supp.2d at 1073-74. This is in contrast to the allegations in the authority cited by defendants on this issue. *See Baba v. Hewlett-Packard Co.*, 2010 WL 2486353 (N.D. Cal. June 16, 2010) (complaint was not sufficient to support liability under the UCL's "unfair" prong as it devoted only a single paragraph to these complex concepts, cursorily listing statutes and alleging vaguely that "HP's conduct offends public policy and is unethical, oppressive, unscrupulous and violates the laws stated...."); *Hodges v. Apple, Inc.*, 2013 WL 6698762, at *9 (N.D. Cal. Dec. 19, 2013) ("Hodges does not identify any law whose policy Apple violated except for vague allusions to deceit, consumer protection, and unfair competition."). Defendants' attempt to analogize such minimal and conclusory allegations to the detailed allegations in plaintiffs' complaint is disingenuous and should be disregarded.

Finally, defendants cite to dicta in *Cullen v. Netflix, Inc.*, 880 F. Supp. 2d 1017, 1028-29 (N.D. Cal. 2012), where the plaintiffs' claim under the unfair prong of the UCL was dismissed. The court noted that plaintiffs did not allege any facts about the potential utility of the challenged conduct, and therefore the court could not conclude that the challenged conduct was immoral or unscrupulous by weighing the utility of the defendant's conduct against the gravity of the harm alleged to the victim. *Id.* In that case, the conduct was Netflix's practice of charging a higher subscription fee for the more accessible (with respect to closed captioning) DVD-by mail plan than for the streaming-only plan. *Id.* Defendants therefore argue that plaintiffs fail to allege facts to support a claim that the gravity of the harm outweighs the utility of the conduct. (Mot. at 41:13-19.) Plaintiffs have, in fact, alleged the purported justification for defendants' conduct, *i.e.*, that it was ostensibly a network diagnostics tool. (SCAC, ¶ 40.) The utility of the diagnostic software as compared to the violations of plaintiffs' privacy rights is discussed in detail in the FTC's investigation and complaint. (SCAC, ¶¶ 75-82.) The FTC concluded that "HTC's practices caused, or are likely to cause, substantial injury to consumers that is not offset by countervailing benefits to consumers or competition . . ." (*Id.*, ¶ 82.) This Court should reach the same conclusion with respect to the purported utility of defendants' conduct. Plaintiffs' allegations therefore state a claim under the "unfair" prong of the UCL, and the motion should be denied.

c. Plaintiffs have pled fraudulent conduct with sufficient detail.

Defendants argue that plaintiffs' UCL claim sounds entirely in fraud. As illustrated in the immediately preceding sections of this memorandum, that is false. But plaintiffs' allegations under the fraudulent-conduct prong of the UCL nevertheless have been pled with sufficient detail.[21]

Plaintiffs have alleged that HTC's User Manuals were deceptive in that HTC represented that through the Android permission-based security model, a user of an HTC Android-based mobile device would be notified when a third-party application required access to the user's personal information or to certain functions or settings of the user's device before the user completed installation of the third-party application. (SCAC, ¶ 79.) In fact, third-party applications could access a variety of sensitive information and sensitive device functionality on HTC devices without notifying or obtaining consent from the user before installation. *Id.*

In addition to the general allegations discussed above, plaintiffs have specifically alleged defendants' failure to disclose. (SCAC, ¶¶ 121-22 (alleging defendants' secret installation of Carrier IQ Software and failure to disclose material information).)

The California Supreme Court has held that non-disclosure is a claim for misrepresentation in a cause of action for fraud. *Kearns*, *supra*, 567 F.3d at 1127 (citing *Engalla v. Permanente Med. Grp.*, 15 Cal. 4th 951, 974 (1997)). Defendants' reliance upon *Marolda v. Symantec Corp.*, 672 F. Supp. 2d 992, 1002 (N.D. Cal. 2009), is misplaced when, as here, the fraud is based upon failure to disclose information that is exclusively within the knowledge of defendants. In *MacDonald v. Ford Motor Co.*, 2014 WL 1340339 (N.D. Cal. Mar. 31, 2014), the Court considered and rejected the very argument made by defendants herein, noting that the facts of *Marolda* were dissimilar because there the dispute concerned alleged omissions within a particular advertisement which plaintiff had failed to produce or adequately describe. *Id.* at *6. Because the content of the advertisement was within

[21] Defendants assert that plaintiffs' UCL claim, as a whole, sounds in fraud, and therefore must satisfy Rule 9(b)'s heightened pleading standards. (Mot. at 37:23-24.) This is not the case, as defendants' own authorities acknowledge. *See Kearns*, 567 F.3d at 1125-26 (noting that fraud is not a necessary element of a claim under the UCL; and, where fraud is not an element of a claim, only allegations of fraudulent conduct must satisfy the heightened pleading requirements of Rule 9(b)). Thus, because each of the three prongs of the UCL state separate theories of liability, only the "fraudulent " prong must satisfy Rule 9(b). The predicate statutes for the unfair and unlawful prong claims herein do not require any misstatements or omissions by defendants to state a claim. Nevertheless, to the extent that the Court finds that the UCL claims and the state consumer protection statutes are all based upon a unified course of conduct, those claims are all pled with sufficient specificity to meet the requirements of Rule 9(b).

the plaintiff's knowledge, she needed to describe the alleged false representation in detail or attach a copy of the offer. *Id*. The court further explained:

> As other courts have recognized, the *Marolda* requirements are not necessarily appropriate for all cases alleging a fraudulent omission. Typically, averments of fraud must be accompanied by the who what when where, and how of the misconduct charged, but claims based on an omission can succeed without the same level of specificity required by a normal fraud claim. This is because a plaintiff alleging an omission-based fraud will not be able to specify the time, place, and specific content of an omission as would a plaintiff in a false representation claim. Because the plaintiffs are alleging a failure to act instead of an affirmative act, the [Plaintiffs] cannot point out the specific moment when the defendant failed to act.

Id. at *6 (citations and internal quotation marks omitted); *see also Baggett v. Hewlett-Packard Co.*, 582 F. Supp. 2d 1261, 1267 (C.D. Cal. 2007) (a claim for fraud by concealment can succeed without the same level of specificity required by a normal fraud claim). [22] Plaintiffs have pled the specific failures to disclose by defendants which are sufficient to place them on notice of the claims asserted. More detail about when and why they decided to withhold this information can be obtained through discovery.

Finally, defendants' argument that plaintiffs have failed to allege a duty to disclose the omitted facts. Defendants argue that for a fraudulent omission claim, the plaintiff must allege a representation made by the defendant that is contrary to the omission of fact that the defendant was obligated to disclose. (Mot. at 39:2-6.) This misstates the law on this issue. The standard is actually that an omission must be contrary to a representation actually made by the defendant, or it must be an omission of fact that the defendant was obligated to disclose. *See Baltazar v. Apple, Inc.*, 2011 WL 588209, at *4 (N.D. Cal. Feb. 10, 2011).

A duty to disclose arises in four circumstances: (1) when the defendant is in a fiduciary relationship with the plaintiff; (2) when the defendant had exclusive knowledge of material facts not

[22] Defendants' other authorities for this argument are therefore inapposite. *See Haskins v. Symantec Corp.*, 2014 WL 2450996 (N.D. Cal. June 2, 2014) (plaintiff's claim was based upon a long-term advertising campaign, yet despite two previous opportunities to amend she failed to identify any specific representations); *Eisen v. Porsche Cars of N. Am., Inc.*, 2012 WL 841019, at *3 (C.D. Cal. Feb. 22, 2012) (plaintiff alleged engine failure due to failure of a shaft or other mechanical failure but failed to allege how the shaft fails, and how that failure will affect the vehicle, what harm the purported defect poses to consumers, or when defendants became aware of the defect); *In re GlenFed, Inc. Sec. Litig.*, 42 F.3d 1541, 1548 (9th Cir. 1994), *superseded by statute on other grounds*, (discussing pleading requirements for misrepresentations and omissions in a securities case); *Kearns*, 567 F.3d at 1126-27 (discussing affirmative misrepresentations some of which were contained in marketing materials).

known to the plaintiff; (3) when the defendant actively conceals a material fact from the plaintiff; and (4) when the defendant makes partial representations but also suppresses some material fact. *Donohue*, 871 F. Supp. at 925. "In an omissions case, omitted information is material if a plaintiff can allege that, 'had the omitted information been disclosed, one would have been aware of it and behaved differently.'" *Ehrlich v. BMW of N. Am., LLC*, 801 F. Supp. 2d 908, 916 (C.D. Cal. 2010) (quoting *Mirkin v. Wasserman*, 5 Cal. 4th 1082, 1093 (1993)). "Materiality is viewed from the prospective of the reasonable consumer." *Ehrlich*, 801 F. Supp. 2d at 916.[23]

Plaintiffs have alleged defendants' duty to disclose. (SCAC, ¶122; *see also* SCAC, ¶¶ 123, 137,146, 153, 179, 217, 260-61, 272, 280, 292, 312 (alleging duty to disclose, defendant's knowledge of the functionality of the software and that this material fact was not known or reasonably discoverable by plaintiffs).) Plaintiffs have further alleged that the plaintiffs would have acted differently if they were aware of the presence of the software on their mobile devices. (*Id.*, ¶ 3.) Thus, plaintiffs have pled a duty to disclose given that (a) the defendants had exclusive knowledge of material facts not known to plaintiffs, and/or (b) defendants actively concealed a material fact from plaintiffs. Defendants' argument—that these allegations are insufficient to the extent plaintiffs have not pled a specific representation actually made by the defendant that is contrary to the allegedly omitted facts—should be dismissed out of hand.[24]

2. Plaintiffs have also stated claims under other state consumer protection statutes.

a. Plaintiffs adequately allege a duty to disclose.

A recurring theme in defendants' arguments against plaintiffs' state consumer protection act claims is the issue of pleading a duty to disclose. Defendants raise this issue with respect to plaintiffs' claims under the Connecticut Unlawful Trade Practices Act ("CUTPA"), Conn. Gen. Stat.

[23] Plaintiffs' fraud-related claim under the UCL is not based upon HTC's failure to deactivate the debug code; however, that failure is discussed in Sec. IV.E below with respect to plaintiffs' breach of warranty claims.

[24] Defendants' authorities on this point are inapposite or contain no more than a summary discussion of rejected concealment claims. *See Tomek v. Apple, Inc.*, 2013 WL 394723 (E.D. Cal. Jan. 30, 2013) (plaintiffs' allegations failed to establish that the defendant ever promised to operate other than it did, and that defendant concealed the purported defect from plaintiff at the time of purchase); *Opperman v. Path, Inc.*, 2014 U.S. Dist. LEXIS 67225, at *19 (N.D. Cal. May 14, 2014) (noting that disclosure claims have failed to allege any information about the warranty on their devices given that a manufacturer's duty to consumers is limited to its warranty obligations absent an affirmative misrepresentation or a safety issue); *see also* Sec. IV.E,2, below, regarding the OEMs' breach of warranty given that the devices are insecure and intercept private and confidential information and data.

§ 42-110a, *et seq.* (Mot. at 42); Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. § 501.201, *et seq.* (Mot. at 43); Maryland Consumer Protection Act ("MdCPA"), Md. Code Com. L. § 13-101, *et seq.* (Mot. at 44); and Michigan Consumer Protection Act ("MiCPA"), Mich. Comp. Laws § 445.901, *et seq.* (Mot. at 45-46). Defendants' primary argument against each of these claims is that plaintiffs do not allege defendants were under any obligation to disclose information regarding the Carrier IQ Software. However, plaintiffs expressly allege a duty to disclose based on defendants' exclusive knowledge of material facts regarding the Carrier IQ Software and partial representations of other facts while omitting or concealing those material facts.[25]

Plaintiffs' allegations satisfy each of the relevant state consumer protection statute's requirements. *See, e.g.*, *Mendelsohn v. BidCactus, LLC*, 2012 WL 1059702, at *6 (D. Conn. Mar. 28, 2012) [CUTPA] ("A duty to disclose arises . . . where a party voluntarily makes some disclosure, as a party who assumes to speak must make a full and fair disclosure as to the matters about which he assumes to speak.") (internal quotations omitted); *Apodaca v. Whirlpool Corp.*, 2013 WL 6477821, at *6-7, 12 (C.D. Cal. Nov. 8, 2013) [FDUTPA] (affirming plaintiff's FDUTPA claim because plaintiff alleged a duty to disclose based on partial representations mixed with suppressions of material fact under the fraud prong of California's consumer protection statutes); *Doyle v. Chrysler Grp. LLC*, 2014 WL 1910628, at *10 (C.D. Cal. Jan. 29, 2014) [MdCPA] (affirming plaintiff's MdCPA claim because plaintiff alleged a duty to disclose based on "material omissions"), *accord* Md. Code Com. L. § 13-301 (expressly defining as "unfair or deceptive trade practices" both

[25] Plaintiffs explicitly allege that "[d]efendants had a duty to disclose the presence and functionality of the Carrier IQ Software" and the "serious privacy violations caused by the Carrier IQ Software." (SCAC, ¶¶ 122, 260-61, 311-12.) They explain that "[t]his duty was based on the fact that only defendants knew of the installation and functionality of the Carrier IQ software," which was a material fact "not known or reasonably discoverable by plaintiffs and the class." (*Id.*, ¶¶ 122-23; *see also id.*, ¶¶ 137, 146, 153, 179, 196, 217, 224, 233, 261, 272, 280, 292, 312.) They further allege that defendants "possessed exclusive knowledge" of the functionality of the Carrier IQ Software and "made incomplete representations about the privacy and functionality of mobile devices generally, and the Carrier IQ Software in particular, while purposely withholding material facts from plaintiffs that contradicted these representations." (*Id.*, ¶¶ 261, 312.) (As needed, plaintiffs request leave to amend to provide further detail of incomplete representations, such as that found in a press release available at http://phandroid.com/2010/03/23/htc-evo-4g-press-release-minisite-now-live/ (last accessed Aug. 19, 2014).) In that press release, HTC (along with Sprint) touted the "full, no-compromise Internet experience" promised by the EVO 4G, without advising customers such as Mr. Szulczewski and others about the presence of the Carrier IQ Software and its functions as complained of in the SCAC, or that his phone would intercept and log copies of his text messages and send them to Google and to HTC itself.) These allegations sufficiently plead a duty to disclose based on defendants' exclusive knowledge of material facts and partial representations of other facts while omitting or concealing those material facts.

"failure to state a material fact if the failure deceives or tends to deceive" and "knowing concealment, suppression, or omission of any material fact . . . ."); *In re Porsche Cars N. Am., Inc.*, 880 F. Supp. 2d 801, 855-56 (S.D. Ohio 2012) [MiCPA] (affirming plaintiff's MiCPA claim for failure to disclose material facts because plaintiff alleged a duty to disclose under California's consumer protection statutes).

The cases cited by defendants are inapposite. In opposing plaintiffs' CUTPA claim, defendants rely on *Putnam Bank v. Ikon Office Solutions, Inc.*, 2011 WL 2633658 (D. Conn. July 5, 2011), where the court found defendant did not owe a duty to disclose that office equipment it had leased to plaintiff contained automatic storage devices that saved images of documents. The court noted that "the essence of the transactions between Putnam and Ikon was the lease of office equipment, not the protection of data that would be saved on the equipment." *Id.* at *3. Conversely, here plaintiffs allege that defendants *actively intercepted and transmitted* their personal and private information, making the essence of the relationship between plaintiffs and defendants more than simply the sale of a mobile device. Defendants' attempt to analogize the facts of *Putnam* to the instant case falls short, as "the essence of the alleged 'transaction' between" plaintiffs and defendants cannot be characterized as "the sale of a Samsung mobile phone, not the handling of consumer data that would be saved on the mobile device." (Mot. at 42-43.)

Against plaintiffs' FDUTPA claim, defendants cite *Virgilio v. Ryland Grp., Inc.*, 680 F.3d 1329 (11th Cir. 2012), where the court affirmed that defendant *developers* (not the builder-seller, as defendants claim) did not owe a duty to disclose to plaintiffs that their residential property was located adjacent to a former World War II bombing site. *Id.* at 1335-38. The holding in *Virgilio*, which considered a judicially created duty tailored to real estate transactions, was based on the unremarkable proposition that there must be "some indicia of privity or a fiduciary, contractual, or other special relationship" between a former home seller and the current buyer "before the duty to disclose can be imposed on a former seller." *Barnext Offshore, Ltd. v. Ferretti Grp. USA, Inc.*, 2012 WL 1570057, at *9 (S.D. Fla. May 2, 2012). That holding is inapplicable here, where plaintiffs allege a direct relationship and attendant duty to disclose between themselves and Carrier IQ and the manufacturers.

b. Plaintiffs adequately allege injury through economic harm.

Another common theme that runs through defendants' arguments is the issue of establishing injury, or economic harm. (Mot. at 46.) Defendants raise this issue with respect to plaintiffs' claims under the CUTPA (no "ascertainable loss of money or property") (*id.* at 41-43); FDUTPA (no "actual damages") (*id.* at 43-44); MdCPA (no "actual injury or loss") (*id.* at 45); and Washington Consumer Protection Act ("WCPA"), Wash. Rev. Code 19.86.010, *et seq.* (no "injury to [plaintiff's] business or property") (Mot. at 51). Defendants' arguments fail here as well because plaintiffs allege specific economic harm that satisfies each of the relevant consumer protection statute's requirements. For example, under the CUTPA, plaintiffs allege they suffered ascertainable loss because they "overpaid for their mobile devices," the value of which has diminished as a result of the Carrier IQ Software's privacy issues and taxing effect on the mobile devices' resources. (SCAC, ¶ 147.) Plaintiffs assert similar allegations of economic harm under the FDUTPA, MdCPA, and WCPA. (*See id.*, ¶¶ 164, 192, 301.) In other areas throughout the SCAC, plaintiffs assert more directly the economic harm they suffered. (*See, e.g.*, ¶ 125 (plaintiffs relinquished "the purchase prices of their mobile devices" and would not have purchased them had they known about the hidden installation and operation of the Carrier IQ Software); ¶ 147 ("The value of [plaintiffs'] mobile devices has diminished now that the privacy issues have come to light, and plaintiffs and the class purchased mobile devices that are not secure and private."); ¶ 182 ("The Carrier IQ Software and the resulting interception and transmission of private information and data to third parties have caused the value of mobile devices to plummet."); ¶ 207 ("This diminution in value [of plaintiffs' mobile devices] amounts to an ascertainable loss of money.").)

Any particularized argument defendants make against plaintiffs' allegations of injury should be rejected. For instance, defendants argue that plaintiffs do not allege "actual damages" under the FDUPTA because they do not plead "the degree to which, or even whether, the market value of any product has changed." (Mot. at 43.) But plaintiffs need not allege at this stage of the case the precise market value of their defective mobile devices. That amount will be determined through discovery and litigated at trial. Additionally, defendants argue that plaintiff Cribbs cannot show "actual injury or loss" under the MdCPA because the Carrier IQ Software was never activated on his

device—even though plaintiffs have pled that they need discovery to understand what "activate" means in this context.[26] (*Id.* at 45.) Finally, defendants argue that plaintiff Sandstrom cannot allege "injury to his business or property" under the WCPA because there is no support for the assertion that defendants' conduct diminished the value of his mobile device. *Id.* at 51. But the case defendants cite, *Cousineau*, is distinguishable on its facts; there, Microsoft's collection of "geolocation" data from plaintiff's phone was insufficient to establish a diminution in value of the phone, while here, defendants' far more egregious privacy violations in the form of intercepting personal, private, and sensitive communications, content, and data beyond mere geolocation information is more than sufficient to demonstrate a diminution in value. (*See also* Secs. A.2 and 4, above, discussing injury-in-fact for purposes of standing.)

c. Defendants' remaining attacks against plaintiffs' consumer protection act claims fail.

Defendants make several additional arguments against certain of plaintiffs' consumer protection act claims. As shown below, none of these arguments has merit.

(1) Plaintiffs allege they relied on defendants' omissions of material fact in purchasing and using their mobile devices for purposes of the MdCPA.

The MdCPA defines "unfair or deceptive trade practices" to include the "failure to state a material fact if the failure deceives or tends to deceive," Md. Code Com. L. § 13-301(3), and the "omission of any material fact with the intent that a consumer rely on the same in connection with: . . . the promotion or sale of any consumer goods, consumer realty, or consumer service." *Id.* § 13-301(9). Omissions are material under the MdCPA "if a significant number of unsophisticated consumers would find that information important in determining a course of action." *Bank of Am., N.A. v. Jill P. Mitchell Living Trust*, 822 F. Supp. 2d 505, 534 (D. Md. 2011) (internal quotations omitted). Additionally, "[a] party seeking to recover damages on a material omission theory under the [MdCPA] must prove reliance." *Id.* "A consumer relies on a material omission under the

[26] In support of their argument, defendants again selectively cite from plaintiffs' allegations regarding AT&T's response to Sen. Franken's letter that the Carrier IQ Software is "embedded" but not "activated" on the Samsung Skyrocket device. (*Id.* at 12 (citing SCAC, ¶ 53).) Defendants, however, ignore the rest of the paragraph, which asserts that "[d]iscovery will help the plaintiffs to understand" AT&T's statement, the interpretation of which cannot be discerned on a motion to dismiss.

[MdCPA] where it is substantially likely that the consumer would not have made the choice in question had the commercial entity disclosed the omitted information." *Id.* at 535.

Defendants do not challenge plaintiffs' allegations that their omissions regarding the Carrier IQ Software were material under the MdCPA. Defendants simply argue that plaintiffs do not sufficiently establish reliance on those material omissions. But defendants' argument that plaintiffs do not identify "any advertisement or statement" upon which they relied misses the mark; plaintiffs need only demonstrate that they "would not have made the choice in question had [defendants] disclosed the omitted information" to establish reliance. *Bank of Am.*, 822 F. Supp. 2d at 535.[27] Plaintiffs do just that, asserting repeatedly that "they would not have purchased their mobile devices had they known that [they] bore hidden battery-, processor-, and memory-taxing software that intercepts private and confidential communications and enables them to be sent to unintended recipients." (SCAC, ¶ 3; *see also, e.g.*, *id.*, ¶¶ 8-25, 137, 146, 170, 182, 217, 224, 233, 280, 292.)

(2) Plaintiffs allege an actionable omission under the MiCPA.

The MiCPA prohibits "unfair, unconscionable, or deceptive methods, acts or practices in the conduct of trade or commerce." Mich. Comp. Laws § 445.903(1). The MiCPA lists 37 different practices as meeting the above standard and being unlawful under the statute. Those practices include: "(c) Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have"; "(e) Representing that goods or services are of a particular standard, quality, or grade . . . if they are of another"; and "(s) Failing to reveal a material fact, the omission of which tends to mislead or deceive the consumer, and which fact could not reasonably be known by the consumer." Contrary to defendants' argument, plaintiffs do specify which of the MiCPA's provisions defendants violated, as they expressly allege under their MiCPA claim that defendants "failed to reveal material facts regarding their mobile devices and the Carrier IQ Software . . . [s]pecifically . . . that the Carrier IQ Software installed on their mobile devices would cause interception and transmission of private information and data, as well as

[27] *See* discussion regarding duty to disclose, above, in Sec. IV.D.

reduced performance and diminished battery life." (SCAC, ¶ 196 (alleging violation of subsection (s).)

Additionally, subsections (c) and (e) are virtually identical to practices proscribed by other state consumer protection acts relevant to this case, including the Rhode Island Unfair Trade Practices and Consumer Protection Act ("UTPCPA"), R.I. Gen. Laws § 6-13.1, *et seq.* Plaintiffs specifically list those provisions in paragraph 248 of the SCAC and allege that defendants violate them. (SCAC, ¶¶ 249-50.) Although plaintiffs do not enumerate those provisions under their MiCPA claim, they need not do so because that claim incorporates by reference their allegations under every other consumer protection act claim. Finally, for the reasons stated above, plaintiffs have alleged an actionable omission because they plead a duty to disclose on the part of defendants.

(3) New Hampshire Consumer Protection Act

The NHCPA has a territorial requirement—the statute prohibits unfair conduct that occurs "within this state." Plaintiffs allege in the SCAC that plaintiff Cline is *currently* a resident of New Hampshire but that at times pertinent to the lawsuit, he lived in Michigan. Plaintiffs incorporate their argument in Sec. A.3, above, regarding standing.[28]

(4) Plaintiffs allege actionable conduct that was a producing cause of their actual damages under the Texas Deceptive Trade Practices Act.

Defendants argue that plaintiffs fail to state a claim under the Texas Deceptive Trade Practices Act ("DTPA"), Tex. Bus. & Com. Code § 17.41, *et seq.*, because they do not allege any of the DTPA's four categories of actionable conduct or that defendants' conduct was a producing cause of actual damages suffered by plaintiffs. These arguments fail. First, plaintiffs sufficiently plead that defendants engaged in a false, misleading, or deceptive act or practice, that they breached an express or implied warranty, and that they engaged in an unconscionable action. *See* Tex. Bus. & Com. Code § 17.50. Under the first "category," the DTPA proscribes a *non-exclusive* list of 27 practices, including "(5) representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have"; "(7) representing that

[28] Alternatively, plaintiffs respectfully request leave to amend to more specifically allege conduct within the state.

goods or services are of a particular standard, quality, or grade . . . if they are of another"; and "(24) failing to disclose information concerning goods or services which was known at the time of the transaction if such failure to disclose such information was intended to induce the consumer into a transaction into which the consumer would not have entered had the information been disclosed." *Id.* § 17.46. As explained above under plaintiffs' MiCPA claim, plaintiffs allege that defendants committed each of these violations. (*See* SCAC, ¶¶ 278-80; *accord, id.*, ¶¶ 248-50.) Under the second "category," the DTPA makes actionable any "breach of an express or implied warranty." Tex. Bus. & Com. Code § 17.50(a)(2). For all the reasons discussed below in Secs. IV.E and IV.F, plaintiffs have successfully pleaded an underlying breach of express and implied warranty claim, satisfying their requirement under the DTPA. Under the third "category," a plaintiff seeking to advance an unconscionable practice claim must establish that the defendant "[took] advantage of the lack of knowledge, ability, experience, or capacity of the consumer to a grossly unfair degree." Tex. Bus. & Com. Code § 17.45(5). Plaintiffs have so established through the allegations in the SCAC, particularly that defendants knew the Carrier IQ Software was installed on consumers' mobile devices, knew its functionality and that it would interfere with plaintiffs' private and sensitive information and data, knew that reasonable consumers would not be able to discover the Carrier IQ Software (and even those who did would not be able to remove it or opt-out of its functions, and failed to disclose all of these material facts. While plaintiffs need only establish *one* of the above categories of conduct to maintain an action under the DTPA, plaintiffs successfully plead actionable conduct under all three categories. *See In re Porsche*, 880 F. Supp. at 876-78 (finding that plaintiffs successfully stated a DTPA claim against Porsche for "misrepresenting the quality of the Cayenne and failing to disclose information about the Cayenne to consumers").

Second, plaintiffs easily show that defendants' conduct was a producing cause of their actual damages. As the Texas Supreme Court held in *Amstadt v. United States Brass Corp.*, 919 S.W.2d 644, 649 (1996) (a case cited by defendants), to be actionable under the DTPA, "the defendant's deceptive conduct must occur in connection with a consumer transaction." This uncontroversial rule, dubbed the "in-connection-with" requirement by the Texas Supreme Court, simply "requir[es] a connection between the plaintiffs, their transactions, and the defendants' conduct." *Id.* at 650.

Plaintiffs here allege that "they would not have purchased or used their mobile devices" had they known about the hidden installation and operation of the Carrier IQ Software. (SCAC, ¶ 280.) That software was designed by Carrier IQ, then installed and implemented by Carrier IQ along with the manufacturers. (*Id.*, ¶¶ 51, 61-63.) Defendants' conduct undoubtedly occurred "in connection with" consumer transactions by which consumers, including plaintiffs, purchased their mobile devices *manufactured by the defendant manufacturers* and containing the Carrier IQ Software *created by Carrier IQ*.

Defendants' reliance on *Amstadt* is unavailing. In *Amstadt*, the court held that plaintiff homeowners could not assert a DTPA claim against manufacturers of plumbing systems because the manufacturers' misrepresentations were not made in connection with the plaintiffs' purchase of their homes. 919 S.W.2d at 650-62. The critical fact in *Amstadt* was that the manufacturers had no role in the consumer transactions at issue—the sale of the homes to the plaintiffs. *Id.* By contrast, here, plaintiffs allege that Carrier IQ, in conjunction with the manufacturers, "intentionally designed and deployed [the Carrier IQ Software] to do far more than gather data regarding signal strength or dropped calls." (SCAC, ¶ 1.) They knew and intended the Carrier IQ Software to be unsuspectingly installed and operating on consumers' mobile devices and designed it *for that very purpose*. (*Id.*, ¶¶ 61-68.) Unlike the manufacturers in *Amstadt*, defendants here played a role in the consumer transactions at issue.

E. Plaintiffs have properly stated claims against the manufacturer defendants for breach of the implied warranty of merchantability.

1. Plaintiffs were not required to give pre-suit notice to the manufacturers; or, in the alternative, the issue of the adequacy of notice given is for the trier of fact.

Plaintiffs brought this claim for breach of implied warranty against the manufacturers ("OEMs"), under the laws of 34 states and the District of Columbia. The OEMs challenge plaintiffs' SCAC only on the basis of a contended failure to give pre-suit notice under six states' laws. Thus, it is only as to these six states where the OEMs have placed notice at issue; as to the others, there is no motion to dismiss on this basis, and plaintiffs' claims under the laws of those other 28 states and the

District of Columbia should not be dismissed.[29] Nor, for the following reasons, should plaintiffs' claims actually addressed by the OEMs' motion be dismissed, either.

"Seller" within the meaning of U.C.C. § 2-607 ordinarily contemplates the direct seller. Defendants concede as much—"[u]nder those states' laws governing implied warranties, plaintiffs must provide reasonable notice of the alleged breach of implied warranty to the *immediate* seller . . . ." (Mot. at 52 (emphasis added).) However, the immediate sellers are not parties to this case. Rather, the OEMs in this case are indirect sellers of the devices (SCAC, ¶ 336); accordingly, no pre-suit notice to them was required to maintain plaintiffs' implied warranty claims under California,[30] Maryland, or Texas law. *Keegan v. American Honda Motor Co., Inc.*, 838 F. Supp. 2d 929, 950-51 (C.D. Cal. 2012); *Firestone Tire & Rubber Co. v. Cannon*, 53 Md. App. 106, 108, 118 (Md. Ct. App. 1982) ; *Vintage Homes, Inc. v. Coldiron*, 585 S.W.2d 886, 888 (Tx. Ct. App. 1979).[31]

With respect to Washington law, there is no reason to believe that it would require any more notice to the defendants than plaintiffs have pled (or of that given by the fact of their filing the underlying and amended complaints in this action). *See Donohue*, 871 F. Supp. 2d at 930 (referring to Washington law's requirement of notice to a "within a reasonable time"; stating that the court could find no authority requiring *pre-suit* notice; and giving leave to amend to show why it was "not unreasonable" to have given notice to defendant after the plaintiff filed suit). Plaintiffs have alleged that the OEMs were on notice from the research and publications of Mr. Eckhart. (SCAC, ¶¶ 41-43, 46.) They also have pled the well-publicized exchange of correspondence with the Electronic Frontier Foundation, extensive press, and reports documenting the breaches involving the OEMs' devices, and government inquiries and investigations as well. (SCAC, ¶¶ 44-45, 47-49, 52-59, 342.)

[29] Furthermore, with respect to plaintiffs' breach of implied warranty claim under the Song-Beverly Consumer Warranty Act, the U.C.C. notification requirements do not apply, and in recognition of such, the OEMs make no challenge on the basis of pre-suit notification. *Mexia v. Rinker Boat Co., Inc.*, 174 Cal. App 4th 1297, 1307 (4th Dist. 2009); *Elias v. Hewlett-Packard Co.*, 950 F. Supp. 2d 1123, 1130 (N.D. Cal. 2013).

[30] As defendants' authority *Lloyd v. Gen. Motors Corp.*, 575 F. Supp. 2d 714, 722 (D. Md. 2008), acknowledged, citing *Firestone*, "[t]he Maryland courts have yet to determine whether a manufacturer . . . may raise as an affirmative defense a consumer's failure to notify his immediate seller of an alleged breach of warranty." In the absence of such authority, the Court should not take the draconian step requested by the defendants, especially in light of the quantum of actual notice that not only the manufacturers received, as discussed immediately below, but that the direct sellers received, too.

[31] Also, in the present case, there are foreign entity defendants for HTC, LG, and Samsung products, along with their American counterparts. Discovery is required to unravel which counterpart defendant did exactly what. A consumer on his or her own could not be expected to know which entity exactly would be a seller for purposes of pre-suit notice.

Further, the public revelations pled by the plaintiffs only brought to light what the OEMs already knew: that the Carrier IQ Software was designed to intercept private communications, content, and data. *They knew this because they wrote the CIQ Interface and installed it alongside the IQ Agent.* Given what they knew and intended with respect to the workings of the Carrier IQ Software, they had direct knowledge that their devices were defective and unmerchantable when they shipped them for sale to consumers. Discovery will further illuminate what the OEMs knew and when they knew it. Finally, as indicated by the OEMs' unyielding approach in this litigation and their continuing demonstration that they are not willing to provide any relief to the plaintiffs, further notice would have been futile in any event. (SCAC, ¶ 342.)

Moreover, the rigid construction of the notice requirement set forth by defendants, especially with respect to non-commercial entities such as the consumer-plaintiffs in this suit, is not contemplated by the U.C.C. As Official Comment 4 to U.C.C. Sec. 2-607 (emphasis added) states:

> The time of notification is to be determined by applying commercial standards to a merchant buyer. *"A reasonable time" for notification from a retail consumer is to be judged by different standards so that in his case it will be extended, for the rule of requiring notification is designed to defeat commercial bad faith, not to deprive a good faith consumer of his remedy.*
>
> *The content of the notification need merely be sufficient to let the seller know that the transaction is still troublesome and must be watched. There is no reason to require that the notification which saves the buyer's rights under this section must include a clear statement of all the objections that will be relied on by the buyer, as under the section covering statements of defects upon rejection (Section 2-605). Nor is there reason for requiring the notification to be a claim for damages or of any threatened litigation or other resort to a remedy. The notification which saves the buyer's rights under this Article need only be such as informs the seller that the transaction is claimed to involve a breach, and thus opens the way for normal settlement through negotiation.*

Especially in light of the policy expressed in this Official Comment, the Court should not dismiss, for the contended failure to give pre-suit notice, plaintiffs' implied warranty claims under California, Maryland, Texas, or Washington law.

2. Plaintiffs' breach of implied warranty claims are properly pled because they have alleged their mobile devices were unmerchantable.

Defendants argue that because plaintiffs' mobile devices are capable of performing the basic functions of making and receiving calls, sending and receiving text messages, and allowing for the use of mobile applications, they have no claim for breach of the implied warranty of merchantability. This argument improperly ignores the confidential, private and secure nature of mobile devices that render them merchantable in the first place. The mobile devices are unmerchantable and not fit for their ordinary purpose since the devices are insecure and intercept private and confidential information and data.

Plaintiffs purchased their mobile devices for the ordinary purpose of performing confidential and private communication via the Internet and with others, via telephone calls and text messages as well as the purchase and use of applications. [32] (SCAC, ¶ 338.) Unfortunately, defendants breached the implied warranty of merchantability by selling mobile devices that contained a latent defect that caused the anticipated uses of the mobile phones to become insecure. (SCAC, ¶¶ 65, 339.) As a result of this breach of privacy, information that the plaintiffs intended to be secure, private and confidential is anything but secure and is being intercepted and shared with third-parties without the plaintiffs' consent. (SCAC, ¶¶ 1, 65, 339, 340.) Thus, the CIQ software prevented these mobile devices from performing their ordinary purpose.[33]

In addition, HTC's and quite possibly other manufacturers' devices contained code that would intercept and transmit the above-referenced content to Google, the manufacturer, and possibly third-party application developers and vendors.[34] (SCAC, ¶¶ 71, 340.) In fact, the FTC discovered during a 2013 investigation that HTC failed to deactivate the "debug code" in the CIQ software. (SCAC, ¶ 77.) As a result, the FTC found that the above mentioned data was accessible to any third-party application. (*Id.*) Clearly, the mobile devices containing CIQ software with the activated "debug code" prevented these mobile devices from performing their ordinary purpose of performing

[32] Within hours of the publication of the defect, consumers expressed their deep concern about the privacy and security violations surrounding Carrier IQ. (SCAC, ¶ 47.)

[33] Also, the Carrier IQ Software depletes the battery power and life of the device, defeating its ordinary purpose. (SCAC, ¶ 341.)

[34] Additional discovery is required to investigate possible other device manufacturers.

confidential and private communication via the Internet and with others, via telephone calls and text messages as well as the purchase and use of applications.

Defendants' attempt to limit the merchantability of the mobile devices to their most basic and simplistic root workings, the ability to make and receive calls, sending and receiving text messages, and the use of mobile applications. However, case law indicates that the implied warranty of merchantability goes beyond the mere operation of the product. *See*, *e.g.*, *Isip v. Mercedes-Benz USA, LLC*, 155 Cal. App. 4th 19, 27 (Cal. Ct. App. 2007) (stating that a vehicle that smells, lurches, clanks and smokes is not fit for its intended purpose merely because it provides transportation from point A to point B); *Stearns v. Select Comfort Retail Corp.*, 2009 U.S. Dist. LEXIS 48367, at *26 (N.D. Cal. June 5, 2009) (holding that the fact that a person may still sleep on a moldy bed does not bar as a matter of law a claim for breach of implied warranty of merchantability); *Montich v. Miele USA, Inc.*, 2012 Dist. LEXIS 41398, at *50 (D.N.J. Mar. 27, 2012) (recognizing that a washing machine's purpose was to wash and clean dirty clothes, but holding that the plaintiffs adequately alleged a breach of implied warranty of merchantability where a machine left clothes smelling like mildew and mold). Thus, merely because the mobile devices may have been able to perform their most basic and simplistic root workings does not make them merchantable. Plaintiffs' mobile devices contain a fundamental defect that made them unfit to use for the ordinary purpose of engaging in *confidential and private* communications via the Internet and via text messages, as well as in the purchase and *confidential and private* use of applications, among other ordinary functions.

Defendants' reliance on *In re iPhone 4S Consumer Litig.* and *Williamson* is misplaced as each is distinguishable from the present matter. In each, the plaintiffs' claims were dismissed for failing to allege that the defect effected the ordinary use of the mobile devices. *See In re iPhone 4S Consumer Litig.*, 2013 WL 3829653, at *16 (N.D. Cal. July 23, 2013) (allegation addressing Siri intelligent assistant feature insufficient because it did not allege that iPhone 4s was deficient in making and receiving calls, sending and receiving text messages or allowing for the use of mobile applications); *Williamson v. Apple, Inc.*, 2012 WL 3835104, at *8 (N.D. Cal. Sept. 4, 2012) (allegations addressing the durability of the glass housing of the iPhone 4 had nothing to do with the

intended use of the smart phone). Unlike *In re iPhone 4S Consumer Litig.* and *Williamson*, plaintiffs' allegations directly affected the ordinary use of plaintiffs' mobile devices. [35]

Thus, plaintiffs' breach of implied warranty of merchantability claims must not be dismissed as they have adequately alleged that the fundamental defect made their mobile devices unfit for their ordinary purpose and unmerchantable.

3. Plaintiffs have sufficiently pled a violation of the implied warranty of merchantability under California Commercial Code Section 2314.

In general, vertical privity is a prerequisite for recovery under Cal. Comm. Code § 2314, California's implied warranty of merchantability. Courts have recognized exceptions to this general rule, including: (1) when the manufacturer engages in conduct directly with the purchaser that functionally places the manufacturer in the position of the direct seller (the "direct dealings" exception) (*Cardinal Health 301, Inc. v. Tyco Elec. Corp.*, 169 Cal. App. 4th 116, 144 (2008)); and (2) when a plaintiff pleads that he or she is a third-party beneficiary to a contract that gives rise to the implied warranty of merchantability (the "third-party beneficiary" exception). *See In re Toyota Motor Corp. Unintended Acceleration Mktg., Sales Practices, & Prods. Liab. Litig.*, 754 F. Supp. 2d 1145, 1184-1185 (C.D. Cal. 2010) ("*In re Toyota Motor Corp.*") ("where plaintiffs successfully plead third-party beneficiary status, they successfully plead a breach of implied warranty claim"); *see also* Cal. Civ. Code § 1559 ("A contract, made expressly for the benefit of a third person, may be enforced by him at any time before the parties thereto rescind it."). Here, in addition to establishing vertical privity by the fact that plaintiffs purchased their mobile devices from actual or apparent agents of the manufacturers, plaintiffs also satisfy both the direct dealings exception and the third-party beneficiary exception to the vertical privity requirement.

Plaintiffs have alleged that they were in vertical privity with the manufacturers in that they purchased their mobile devices from actual or apparent agents of the manufacturers, such as the

[35] Further, defendants' reliance on *Tomek v. Apple, Inc.*, is also misplaced as it is distinguishable from the present matter. In *Tomek*, the court found that plaintiff's claim that his computer's battery only shut down once during a unique situation was insufficient to show that the computer was not fit for ordinary use. 2012 WL 2857035, at *7 (E.D. Cal. July 11, 2012). Plaintiffs do not allege that the fundamental defect only made their phone unmerchantable during one unique circumstance. Rather, plaintiffs have alleged that during the entire life of their phones the fundamental defect depleted their battery power and diminished the lives of the devices. (*See* SCAC, ¶ 341.)

manufacturers' authorized dealers. (SCAC, ¶ 336); *see also Cardinal Health 301, Inc.*, 169 Cal. App. 4th at 138 ("Vertical privity means that the buyer and seller were parties to the sales contract."). Under California law, an agent is "one who represents another, called the principal, in dealings with third persons." Cal. Civ. Code § 2295. An "ostensible agency" is formed when the principal "intentionally, or by want of ordinary care, causes a third person to believe another to be his agent who is not really employed by him." Cal. Civ. Code § 2300. Whether plaintiffs purchased their mobile devices from agents of the manufacturers is a question of fact reserved for the jury. *See Garlock Sealing Techs., LLC v. NAK Sealing Techs. Corp.*, 148 Cal. App. 4th 937, 965 (2007) ("The existence of an agency relationship is a factual question for the trier of fact"); *see also Holt v. Kormann*, 2012 WL 2150070 (C.D. Cal. June 12, 2012) (denying motion to dismiss agency claim where the purported agent's use of names and logos and the existence of a business relationship between the two entities made an ostensible agency relationship plausible).

In addition, plaintiffs have alleged facts sufficient to state a claim of violation of implied warranty based on the direct dealings exception to the privity rule established in *U.S. Roofing, Inc. v. Credit Alliance Corp.*, 228 Cal. App. 3d 1431, 1442 (Cal. Ct. App. 1991). *See Cardinal Health 301, Inc.*, 169 Cal. App. 4th at 139-45 (analyzing the holding in *U.S. Roofing* and concluding that where the manufacturer adopts and benefits from the sales negotiations between another party and the buyer, and there are direct dealings between the parties, the requisite privity for purposes of establishing an implied warranty is established). Here, plaintiffs allege that the manufacturers provided written warranties in conjunction with the purchase of their mobile devices, and these written warranties are enforceable by plaintiffs and the class against the manufacturers regardless of where or from whom the mobile devices were purchased. (SCAC, ¶ 337.) Because the manufacturers essentially adopted and benefited from the sales negotiations that took place when plaintiffs purchased their mobile devices, and because the manufacturers provided written warranties enforceable by plaintiffs against the manufacturers, the manufacturers have engaged in conduct with the plaintiffs that "functionally places the [manufacturers] in the position of the direct *seller*." *Cardinal Health 301, Inc.*, 169 Cal. App. 4th at 144.

Finally, plaintiffs allege that they were intended third-party beneficiaries of the manufacturers' contract for sale of devices to the persons or entities from whom plaintiffs and the class ultimately purchased their mobile devices. (SCAC, ¶ 337.) Thus, plaintiffs have stated a claim against the manufacturers for breach of the implied warranty of merchantability. *See In re Toyota Motor Corp.*, 754 F. Supp. 2d at 1185 ("Plaintiffs have pled that they purchased vehicles from a network of dealers who are agents of Defendants. … Like the plaintiffs in *Gilbert*, *Cartwright*, and *In re Sony VAIO*, plaintiffs allege they were the intended consumers. Like those plaintiffs, they allege facts tending to support that they are third-party beneficiaries; therefore, plaintiffs' breach of implied warranty claim is not precluded by the lack of vertical privity.").

Citing *Clemens v. DaimlerChrysler Corp.*, 534 F.3d 1017, 1023 (9th Cir. 2008), defendants contend that the claim made under Cal. Comm. Code § 2314 should be dismissed because the complaint is "lacking sufficient allegations to establish vertical privity" (Mot. at 56-57) and plaintiffs have not pled exceptions to the vertical privity requirement. (Mot. at 57 n.20.) The court in *In re Toyota Motor Corp.* considered and rejected a similar argument. There, plaintiffs sued Toyota, the manufacturer of vehicles alleged to be defectively designed, and pled that they purchased the vehicles from dealers who were agents of Toyota. 754 F. Supp. 2d at 1185. Plaintiffs also pled that "the warranty agreements [between Toyota and the dealers] were designed for and intended to benefit the ultimate consumers only." *Id*. Nonetheless, Toyota argued that plaintiffs could not recover under the implied warranty of merchantability because plaintiffs were not in vertical privity with Toyota. *Id*. The court disagreed, explaining that "the clear weight of authority compels a conclusion that where plaintiffs successfully plead third-party beneficiary status, they successfully plead a breach of implied warranty claim." *Id*. at 1184. The court also explained that "Toyota's reliance on *Clemens v. DaimlerChrysler Corp.*, […], a Ninth Circuit case applying California law, neither compels nor counsels a contrary result" because "the court [in *Clemens*] did not consider the third-party beneficiary exception to the vertical privity requirement." *Id*. at 1185.

The same result is required here. Plaintiffs have sufficiently pled breach of implied warranty under California law for the three above-stated reasons. Thus, defendants' motion to dismiss this claim should be denied.

4. Plaintiffs' Song-Beverly Act claims are properly pled because multiple plaintiffs allege purchases within California.

Defendants wrongly assert that all plaintiffs' claims under the Song-Beverly Act should be dismissed for failure to plead a sale within California. But defendants' own submissions in support of their motion to compel arbitration (Dkt. No. 129) show that defendants have been on notice of where each plaintiff purchased his or her device since at least 2012, through records they obtained from the wireless carriers. (*See* Dkt. No. 129.) In fact, defendants submitted sworn declarations affirming that California resident plaintiffs purchased their devices in California. (*See* Declaration of Chenell Cummings (Dkt. No. 132), ¶ 11 ("[Plaintiff] Daniel Pipkin purchased an Apple iPhone from an AT&T retail store in Oxnard, California . . . and then purchased a Samsung Galaxy S II Skyrocket SGH-i727 from that same store . . . ."); Declaration of Stephanie Miller (Dkt. No. 135), ¶ 21 ("[O]n July 28, 2010, [plaintiff Dao Phong] upgraded to an Evo phone, manufactured by HTC, through an indirect dealer, FoneArt Communications.").[36]) Accordingly, defendants' citations to cases where plaintiffs neither resided in California, nor claimed to have purchased a product there, are entirely inapposite. *See, e.g.*, *Elias v. Hewlett-Packard Co.*, 903 F. Supp. 2d 843, 851 (N.D. Cal. 2012).

Further, plaintiffs Phong, Pipkin, and Patrick all reside in California, and the SCAC limits its Song-Beverly Act claims to "plaintiffs and the other class members who purchased mobile devices in California." (SCAC, ¶¶ 9–11, 353.) Their California residency is a sufficient basis from which defendants and the Court may reasonably infer that their devices were sold in California. *Cf. Montich v. Miele USA, Inc.*, 849 F. Supp. 2d 439, 455 (D.N.J. 2012) (denying motion to dismiss Song-Beverly Act claims where plaintiff did not specifically plead she bought her washing machine new, but "it is reasonable to infer [from the purchase price] she was not purchasing a second-hand washing machine"). This is especially true since defendants have demonstrated they actually possess knowledge of where each device was purchased.

[36] Based on plaintiffs' research, FoneArt Communications is an unincorporated business entity operating as a Sprint phone dealer with retail locations solely in the area of San Francisco, California, including in San Francisco, Oakland, and San Jose. If needed, plaintiffs respectfully request leave to amend to include the specific purchase place for Ms. Phong's phone, as well as that of plaintiff Jennifer Patrick, another California resident who purchased her device in Sacramento at an AT&T store. *See, e.g.*, *Kowalski v. Hewlett-Packard Co.*, 771 F. Supp. 2d 1138, 1156 (N.D. Cal. 2010) (granting motion to dismiss Song-Beverly Act claim with leave to amend).

F. Plaintiffs have stated claims under the Magnuson-Moss Warranty Act.

For all the reasons stated above, plaintiffs have sufficiently pled implied warranty claims under the laws of multiple states, and they have, therefore, sufficiently pled violations of the Magnuson-Moss Warranty Act. "As courts have concluded, the statute provides a federal cause of action for state law implied warranty claims." *In re ConAgra Foods, Inc.*, 908 F. Supp. 2d 1090, 1102 (C.D. Cal. 2012); 15 U.S.C. §§ 2301(5), 2310(d)(1). The sole ground defendants raise to dismiss plaintiffs' Magnuson-Moss Act claims is plaintiffs' alleged failure to state implied warranty claims under state law. The cases defendants cite, however, do not raise any issue not already discussed herein, and none discuss implied warranty claims under the laws of any state other than California.[37] Because plaintiffs have adequately pled state law implied warranty claims and defendants have set forth no other basis to dismiss plaintiffs' Magnuson-Moss Act claims, the motion to dismiss must be denied. *Horvath v. LG Elecs. MobileComm U.S.A., Inc.*, 2012 U.S. Dist. LEXIS 19215, at *23–25 (S.D. Cal. Feb. 13, 2012) (denying motion to dismiss Magnuson-Moss Warranty Act claims where plaintiff "alleged facts sufficient to raise his right to relief for violations of the Song-Beverly Warranty Act above the speculative level"); *Tait v. BSH Home Appliances Corp.*, 2011 U.S. Dist. LEXIS 103584, at *15 (C.D. Cal. Aug. 31, 2011) (denying motion to dismiss Magnuson-Moss Warranty Act claims where "[t]he sole grounds offered by Defendant . . . is the assertion that plaintiffs have failed to plead a valid warranty claim under the laws of any state").

[37] In *Soars v. Logrono*, 2014 U.S. Dist. LEXIS 24674, at *13 (N.D. Cal. Feb. 25, 2014), the *pro se* plaintiff alleged simply a breach of implied warranty "'as required by statutes in the state of California and the Magnuson-Moss Warranty Act'" without further elaboration. The court dismissed the plaintiff's implied warranty claims for failure to plead vertical privity as to claims based on the California Commercial Code and failure to plead that the plaintiff was a "buyer" protected by the Song-Beverly Act. *Id.* at *14-16. The court, therefore, also dismissed the plaintiff's Magnuson-Moss Act claims in a footnote without further discussion. *Id.* at *16-17 n.3. No other state's implied warranty law or other basis for implied warranty claims were discussed. *See also In re Sony Grand WEGA KDF-E A10/A20 Series Rear Projection HDTV TV Litig.*, 758 F. Supp. 2d 1077, 1100 (S.D. Cal. 2010) (dismissing Magnuson-Moss Act claims where there were multiple pleading deficiencies as to California implied warranty claims, plaintiffs failed to allege products were purchased in California for Song-Beverly Act claims, and no other state's implied warranty laws were at issue). *Tavion Commc'ns, Inc. v. Ubiquity Networks*, 2014 U.S. Dist. LEXIS 35455 (N.D. Cal. Mar. 14, 2014), did involve implied warranty claims under the laws of multiple states. There, the court dismissed the plaintiffs' Magnuson-Moss Act claims due to the "more fundamental defect," however, that the products at issue were not "consumer products" under the MMWA and the plaintiffs were not "consumers." *See id.* at *34-40; 15 U.S.C. § 2310(d)(1). Defendants here do not challenge that plaintiffs are consumers under the Magnuson-Moss Act, and the *Tavion* case is thus inapposite.

V. CONCLUSION

For all of the foregoing reasons, defendants' motion should be denied in its entirety. Further, as necessary to avoid dismissal of any of their claims, plaintiffs respectfully ask that their requests for leave to amend be granted.

Dated: August 21, 2014.

HAGENS BERMAN SOBOL SHAPIRO LLP

By: */s/ Steve W. Berman*
Steve W. Berman (*pro hac vice*)
Robert F. Lopez (*pro hac vice*)
1918 Eighth Avenue, Suite 3300
Seattle, WA 98101
Telephone: (206) 623-7292
Facsimile: (206) 623-0594
steve@hbsslaw.com
robl@hbsslaw.com

PEARSON SIMON &WARSHAW, LLP

By: */s/ Bruce L. Simon*
Bruce L. Simon (CSB No. 96241)
Robert G. Retana (CSB No. 148677)
44 Montgomery Street, Suite 2450
San Francisco, CA 94104
Telephone: (415) 433-9000
Facsimile: (415) 433-9008
bsimon@pswlaw.com
rretana@pswlaw.com

Daniel L. Warshaw (CSB No. 185365)
15165 Ventura Blvd., Suite 400
Sherman Oaks, CA 91403
Telephone: (818) 788-8300
Facsimile: (818) 788-8104
dwarshaw@pswlaw.com

Plaintiffs' Interim Co-Lead Counsel

J. Paul Gignac
ARIAS OZZELLO & GIGNAC LLP
115 S. La Cumbre Lane, Suite 300
Santa Barbara, California 93105
Telephone: (805) 683-7400
Facsimile: (805) 683-7401
j.paul@aogllp.com

Rosemary M. Rivas
FINKELSTEIN THOMPSON LLP
505 Montgomery Street, Suite 300
San Francisco, California 94111
Telephone: (415) 398-8700
Facsimile: (415) 398-8704
rrivas@finkelsteinthompson.com

Eric D. Holland
HOLLAND GROVES SCHNELLER STOLZE LLC
300 N. Tucker Blvd., Suite 801
Saint Louis, MO 63101
Telephone: 314-241-8111
Facsimile: 314-241-5554
eholland@hgsslaw.com

Paul R. Kiesel
Jeffrey A. Koncius
Mariana Aroditis
KIESEL BOUCHER LARSON LLP
8648 Wilshire Boulevard
Beverly Hills, CA 90211
Telephone: (310) 854-4444
Facsimile: (310) 854-0812
kiesel@kbla.com
koncius@kbla.com
maroditis@kbla.com

Charles E. Schaffer
LEVIN, FISHBEIN, SEDRAN & BERMAN
510 Walnut Street, Suite 500
Philadelphia, PA 19106
Telephone: (215) 592-1500
Facsimile: (215) 592-4663
cschaffer@lfsblaw.com

Executive Committee Members for the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on August 21, 2014, I electronically filed the foregoing document using the CM/ECF system which will send notification of such filing to the e-mail addresses registered in the CM/ECF system, as denoted on the Electronic Mail Notice List, and I hereby certify that I have caused to be mailed a paper copy of the foregoing document via the United States Postal Service to the non-CM/ECF participants indicated on the Manual Notice List generated by the CM/ECF system.

Dated: August 21, 2014

/s/ *Steve W. Berman*
Steve W. Berman

ATTESTATION PURSUANT TO LOCAL RULE 5-1(i)(3)

I, Steve W. Berman, am the ECF User whose identification and password are being used to file this **Plaintiffs' Memorandum In Opposition to Defendants' Motion To Dismiss**. In compliance with Civil Local Rule 5-1(i)(3), I hereby attest that all signatories have concurred in this filing.

Dated: August 21, 2014

/s/ *Steve W. Berman*
Steve W. Berman